Started on Jan 29th 2021.

SAP GRC: Governance Risk and compliance

1) It's a compliance tool
2) The purpose of GRC tool is to control financial frauds/Risks
3) How this is introduced into the market?

   Enron Corporate scandal happened in 2001.

   Satyam Corporate Scandal happened in 2008.

Due to this Scandal, SAP has come up with SAP GRC to control Financial frauds in the Organizations.

What SAP did was it took 3rd party tool VIRSA in 2006 and renamed it as GRC

- SAP GRC Versions: GRC 5.0,5.1,5.2,5.3 (SAP GRC 5X Series)
- Its installed on top of SAP NW application server JAVA, JAVA based component/Application.
- GRC is a component-based application. (Even IDM also component-based application)
- Later GRC introduced 10.0,10.1 (SAP GRC 10X Series)
- Its installed-on top of SAP NW application server ABAP
- It's a ABAP based application

SAP GRC SUITE: It has many applications in it (7)

SAP Business suite: ECC, CRM, SRM, SCM

SAP GRC SUITE:

1) Access Control
2) Process Control
3) Risk Management
4) NFE
5) GTS
6) Fraud Management (Added Newly)
7) Audit Management (Added Newly)

Audit Management:

- Used for Auditing Purpose.
- We have Broader functionalities related to Audit.
- Earlier we used AC for Auditing (Providing reports to Business/Audit team)
- Now it’s a separate Application where we have more functionalities
- We have 2 types of Auditing’s (System Auditing, Business Auditing)
- SAP charges you the application based on the no of users. This is called Technical Auditing.
- Technical Auditing means Licensing related.
- We don’t get involve in Business Auditing. We are not responsible for this.

Fraud Management: We can control frauds in company

GTS: Global Trade System

You are in USA and you want to establish a company in India. As per India rules, you can not directly establish a company and you have to tie up one with Indian company and you will have 49% Share and Indian company have 51%

NFE: Nota Fiscal Electronica

This NFE specially designed for Brazil companies.

- When we purchase a particular product, We get the Invoice after the payment.
- This invoice should be sent to Govt for Taxation
- It depends on country to country sending invoice to Govt (Quarterly/Half Year/Year)
- But in Brazil, Invoice should be sent to Govt on the same day of transaction.SO there is no chance of tax manipulation.
- In India , we generally manipulate the taxes as we get more time.
- NO other company/client use NFE other than Brazil.

Risk Management:

Every Organization will have one department called “ Risk Management”.

Eg: Physical theft, Natural disasters, fire and safety comes under this.

Process Control:

- Its one of the Imp app of GRC Suite
- All the process of organizations that is rule and regulations defined in PC.
- This is used by Business Team
- AC and PC are interrelated with each other.
- We technically work in Ac whereas Business team works in PC.

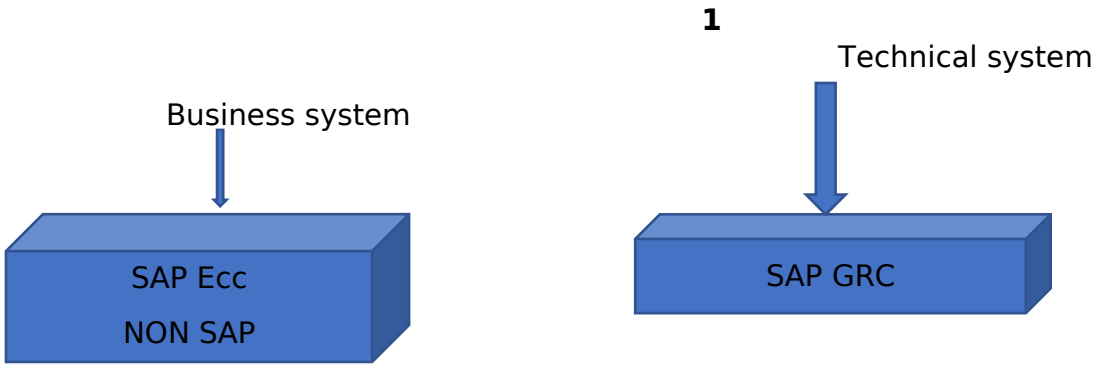
Access Control:

- Purpose of AC is to provide the access to Business users
- We control the access of users.
- SOD- Segregation of Duties
- SOD says one individual should not have complete control over a process.
- If there is a not complete control, there is a chance of risk. When there is chance of risk, there a chance of fraud.
- Eg: Su01, Pfcg
- If one has access to both T-codes, he can create a sensitive/Critical role and he can assign to himself /anyone which is a risk.

We can use su01, other T-codes via web browser also. But we need to configure Web Browser for that.

It has 4 components/Sub Application in it

GRC 10x	**GRC5x**
1) ARA (Access Risk Analysis)	**RAR (Risk Analysis Remediation)**
2) ARM(Access Request Management)	**CUP(Compliant User Provisioning)**
3) BRM(Business role Management)	**ERM(Enterprise Role Management)**
4) EAM(Emergency Access Management)	**SPM(Super Privilege Management)**



Business System: We perform Business operations.

Technical system:

1) We don't perform any Business operations.
2) Its used to accelerate the Business application.
3) Other examples: Solman and Portal(We do not perform any Business activities)

ARA

1) We can perform risk analysis in the Business system.
2) For ex, we have 1000 users in Ecc and 100 users have risk
3) Out of 100, 50 are sales department, 50 are Finance department
4) Once we found this, we need to submit this report to Sales , Finance Departments.
5) Now, its their call what to do with these users.
6) There are 2 options form them. Either they can **remediate** the risk or **Mitigate** the risk

Remediation: Removing risk/confliction T-code

Mitigation: Allowing the risk to user is called Mitigation.

What happen if we mitigate the user.? There is a chance he can mis use the access. So, we have to monitor the activities of the user.

So, we have a person who is the responsible to monitor the activities of mitigated user.

ARA is a mandatory component when you are implementing GRC AC

With Out ARA, we cannot use AC. Other components are up to org requirement. But ARA is must.

ng GRC AC.

ARM

1) We provide access to users via ARM.
2) We can perform all user administrative activities.
3) We can do this via Su01 in Ecc system. But , its manual process.
4) With ARM, We can make user administration automated.
5) We can also implement approval process using ARM.
6) We are creating GRC Requests for all activities(User creation/Change/Lock/Un lock/Delete)
7) Once GRC Req created, it goes to approver and once approver approves, needful action will be performed in backend system
8) We need to Implement MSMP Workflow for ARM
9) ARM is complete automated process for Su01

BRM

1) Purpose of BRM is to maintain the roles.
2) We can maintain roles via PFCG as well. But , it's a manual process.
3) Advantage of BRM is , We are going to maintain Risk free roles.
4) For ex, if you are creating a role via pfcg with critical T-codes for Basis like (RZ10, Se38, SM59, STMS, SM30), pfcg will not warn you having these T-codes in a single role causing risk and it will allow you to create.
5) Where as BRM will warn you. Risk analysis will be performed before role is created.
6) In Risk analysis, if we found HIGH risks, it has to be approved by role owner.
7) When there is no Risk at role level, there is no risk for users aswell.

EAM

1) When a user needs to perform additional activities for which he does not have access, then user can go for EAM for limited period.
2) We have 4 types of users in EAM

- **Firefighter**: Who seeks additional access. (Venkatesh)

- **FF ID**: it’s a user id which will have required additional access. (E_SE_GBL1) will be assign to Firefighter.
- **FF Owner**: There must be FFOwner for each FFid who is responsible to allow this FFID to Firefighter.(Evandro)
- **FF Controller**: Activities done by Firefighter will be monitored by FF Controller.

MSMP Workflow: (Multistage Multi Path)

- We can implement for MSMP for ARM, ARA, BRM, EAM
- Its not mandatory to configure MSMP for ARA, BRM, EAM
-

But its mandatory for ARM.

- We cannot use ARM, With our implementing MSMP.
- Its most Important and difficult concept to understand in GRC AC.
-

Installation of SAP GRC

- When we install SAP GRC , by default we get AC/PC/RM applications
- If we want other applications(GTS, NFE, Audit management...), need to install components separately
- Installation will be done by Basis Team.
- Coming to Installation, We need to install SAPNW AS ABAP 7.02.
- Then , we need to install GRCFND_A(GRC Foundation ABAP) Component.
- By installing this GRCFND_A, we will get 3 applications AC, PC, RM

Note: To identify whether GRC system is 10/10.1 version

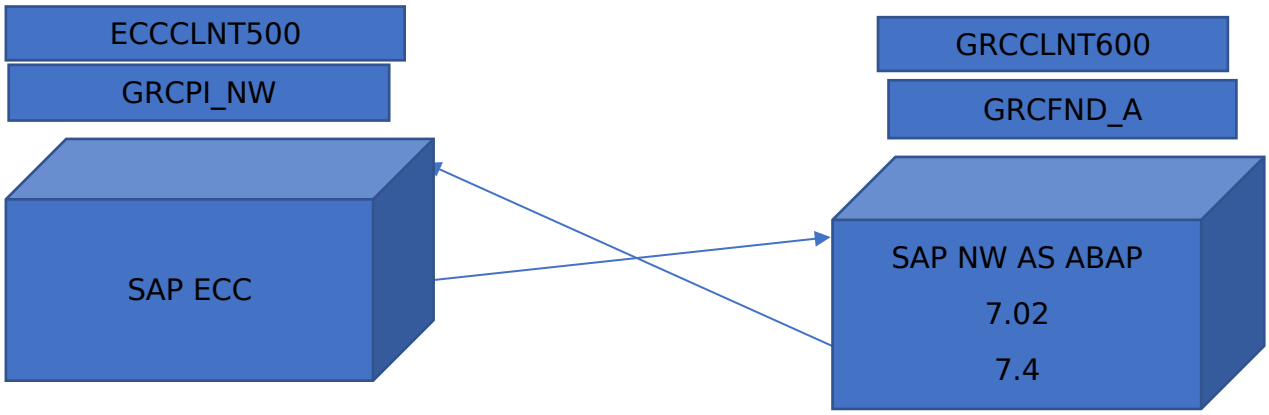
If we found GRCFND_A V1000 ---- GRC 10

GRCFND_A V1100---GRC 10.1

GTS- **SLL LEG component**

NFE – **SLL-LFE Component**

1) This is main job of Basis team



2) Minimum version is 7.02 for NW AS ABAP to install SAP GRC
3) Main Installation components:
   GRCFND_A V1000 GRC Foundation ABAP

4) SAP NW AS ABAP 7.02 with SP6 or Higher

SAP GRC 10.1

SAP NW AS ABAP 7.40 SP02

GRCFND_A V1100

- We also have plug in components
- Based on the backend system, we also need to install plug
- We need to install Plugins via SAINT T-code or SUM tool.

Create client in GRC, ECC (SCC4)
Client copy of both new clients(SCCL)
Establish RFC connection between 2 new clients
Login With SAP* in new clients
Create one own super user

Configuration of GI

- We have 2 systems. SAP ECC, GRC
- We need to have 2 clients.
- We are establishing connection between ECC , GRC us
  Function Call)
- We need to have 2 separate clients for 2 systems.
- Each client is treated as Logical system in live environment
- We do not use multiple clients in single system in live environment.
- Create a new client in GRC with SCC4
- Login with SAP* and pass in new client
- We can login only with SAP*
- We can not perform any activity. Because, it does not have any data.
- So, we need to perform client copy (SCCL)
- Select SAP_CUST always
- Source client is 000 and schedule as back ground Job.
- We can check the status via SCC3
- It takes 15-20 mins/More to copy the data from 000 client to newly created client.

  Note: In Realtime scenario, Basis team provide us client details and establish RFC connection and hand over the system to Security.

  RFC Communication Process:
  We need to perform below steps in both GRC, ECC Systems

1) Define Logical system BD54/SALE---□ (SALE---Basic Settings---Define Logical system—New Entries—ECCCLNT700) Capital letters only----it asks for TR
2) Assign Logical system to Client SCC4/SALE ((SALE---Basic Settings---Assign Logical system to Client—Double client on Client & Save.
3) Create a user for communication SU01
4) Establish RFC Communication SM59/SALE(SALE---Communication---Create RFC Connections) or SM59----click on " Create"
   RFC Destination: If you are in ecc, GRCCLNT700 and If you are in GRC, ECCCLNT700 and connection type 3.
   Description: Connection from Ecc to GRC and ENTER
   Now "**Technical settings**" will be opened/enables
   Target Host: (System—Status—Servername) --**sapsystem** (sapsystem_ECC_10)
   Instance:(System—Status—Servername) **10**

Logon and Security:

Client: Target system client
User: Target system user id created for RFC
Password:
And save.

But how can we make sure connection is established successfully?

Utilities-□ Test-□ Connection Test
Utilities-□Test-□Auth Test (To make sure that given user in " Logon and Security" has required access for Communication

Note: If you give wrong Host name, IP address will not be shown

We need to establish communication from
ECC--□GRC
GRC--□ECC

Create a RFC user:

- Su01 and user type " SYSTEM"
- Need to provide required role(s) for Communication.
- There is one role which provides only communication auth. Need to assign this.

Now, Implementation and Configuration will starts

We have total 14 steps to configure SAP GRC
When we install SAP GRC , by default we get AC/PC/RM applications.
If we want other applications(GTS, NFE, Audit management…), need to install components separately.
If we perform these 14 steps by our own, we can be part of GRC Implementation project.

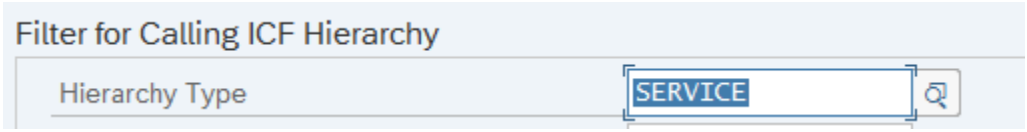
1) Most of the Configuration activities of GRC AC done in SPRO in GRC.
2) There are total ---- steps .
   - Activate Applications
   - Activate SICF Services
   -

1) Activate Applications:

- Login to GRC system.
- Execute SPRO and go to below path
- SAP Reference IMG--□ GRC….> General Settings-□ Activate Applications in client.
- By default, AC, PC, RM activated. But, based on requirement, Activate required Component. Ex Activate AC.
- Save it and it will ask you TR and create a new TR. (Are we doing it in GRC Dev and moving TR to GRC Prod?) or making changes directly in GRC Pord?(Ans : GRC DEV and TR should be moved.)

Question: How to activate only ARA/EAM in AC. I don't need ARM, BRM.

2) Activate SICF Services:

- We do this via SICF T-code (SAP Internet Communication Framework)
- By Activating SICF Service, we will get required networking https, Https web services required for GRC system.
- 

  and execute.
- Default host-□SAP-□GRC and right Click and " Activate Service"
- There are so many sub notes which are to be activated.
- /SAP/Public/BC(all subnotes should activated)
- /SAP/Public/BC/Icons (all subnotes should activated)
- /SAP/Public/BC/Icons/rtl(all subnotes should activated)

- /SAP/Public/BC/its(all subnotes should activated)
- /SAP/Public/BC/pictrograms(all subnotes should activated)
- /SAP/Public/BC/ur(all subnotes should activated)
- /SAP/Public/BC/Webdynpro(all subnotes should activated)
- /SAP/Public/BC/Webdynpro/Mimes(all subnotes should activated)
- /SAP/Public/BC/Webdynpro/Adobechallange(all subnotes should activated)
- /SAP/Public/BC/Webdynpro/ssr(all subnotes should activated)
- /SAP/Public/BC/webicons(all subnotes should activated)
- /SAP/Public/SSOCNTL(all subnotes should activated)
-

After activating these services , we need to publish them with below T-code

T-code: SIAC_publish_all_internal

After publish only, services will be available.

Publishing means we are releasing it.

All the activated services will be published once executed.

Question: If we forget to activate service, will it be published?

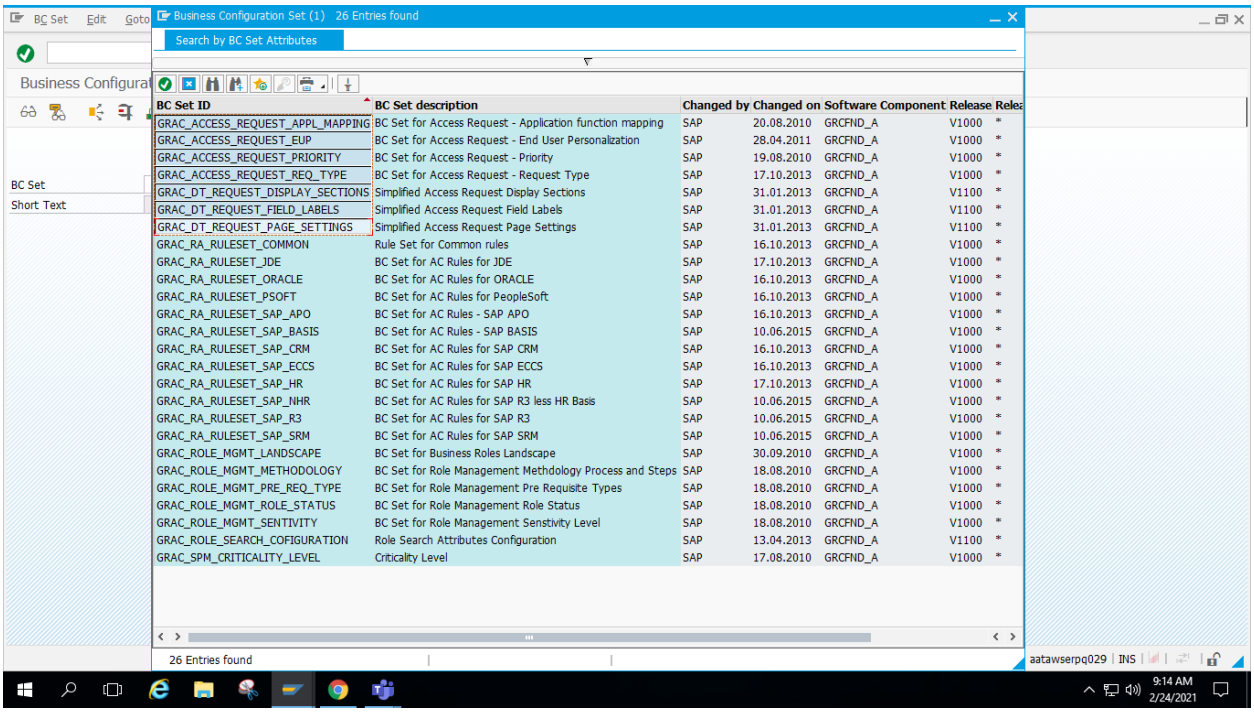
Note1 : It's a cross client activity. If we activate in once client, activated in other clients as well

Note2:Activate SICF Services:There are almost 200 notes to be activated as aprt of 2nd step (Activate SICF Services😊
Its almost take 1 to 2hours to activate all these.

3) **Activate BC Set:**

- We can activate BC Set via T-code **SCPR20**
- BC Set----Business Configuration set
- BC set provides standard settings, standard tables, standard data required for AC.
- We need to activate only *GRAC* BC sets.
- There are BC sets for each component (ARA, ARM, BRM, EAM)
- The rule to activate BC sets is , 1st we have to activate ARA BC Set.
- GRAC_RA_RULESET_COMMON should be activated 1st. Standard tables, standard data required for ARA will be available once you activate this BC SET.later we don't need to maintain any sequence.
- ARA --1 BC Set (1 in GRC 10.1) GRAC_RA_RULESET_COMMON
- ARM-4 BC Sets(7 in GRC10.1)
- BRM-5 BC Sets (6 in GRC 10.1)
- EAM- 1 BC Set (1 in GRC 10.1)

BC SETS of AC



ARM BC SETS: 7 ((GRC10.1))

GRAC_ACCESS_REQUEST_APPL_MAPPING

GRAC_ACCESS_REQUEST_EUP

GRAC_ACCESS_REQUEST_PRIORITY

GRAC_ACCESS_REQUEST_REQ_TYPE

GRAC_DT_REQUEST_DISPLAY_SECTIONS

GRAC_DT_REQUEST_FIELD_LABELS

GRAC_DT_REQUEST_PAGE_SETTINGS

BRM BC SETS: 6 (GRC10.1)

GRAC_ROLE_MGMT_LANDSCAPE

GRAC_ROLE_MGMT_METHODOLOGY

GRAC_ROLE_MGMT_PRE_REQ_TYPE

GRAC_ROLE_MGMT_ROLE_STATUS

GRAC_ROLE_MGMT_SENTIVITY

GRAC_ROLE_SEARCH_COFIGURATION

EAM BC SET: 1 ((GRC10.1)

GRAC_SPM_CRITICALITY_LEVEL

Backend System (ECC) BC SET:

GRAC_RA_RULESET_SAP_R3

- Its Single time activity.
- You can check the logs as well whether activated successfully or not.
- We may get yellow, Red, Green symbols and below are meaning
- Yellow: A Message with Yellow background, it just warning and you can proceed.
- Red: A Message with Red background, you must resolve this.
- If you receive a Basis error message with Red background, please contact system Administrator.
- BC Set activation is not cross client. Means, its client independent. If we activate in 1 client, it will not go to another client.

- At last , we need to activate Backend system(ECC/SRM/CRM) BC Set. It takes some time compare other BC set activation. It has 8 Packages.
- GRAC_RA_RULESET_SAP_R3 is the BC Set for ECC.

Note 1: Always use expert mode when you are activating BC SET. This is SAP's Suggestion. Because, if there is any change required, system it self will take care.

Note 2: The rule to activate BC sets is , 1st we have to activate ARA BC Set(What if we activate other BC Set)

Eg: If we activate GRAC_ACCESS REQUEST_REQ_TYPE, different req types like, creating, change, delete, lock , unlock will be available.

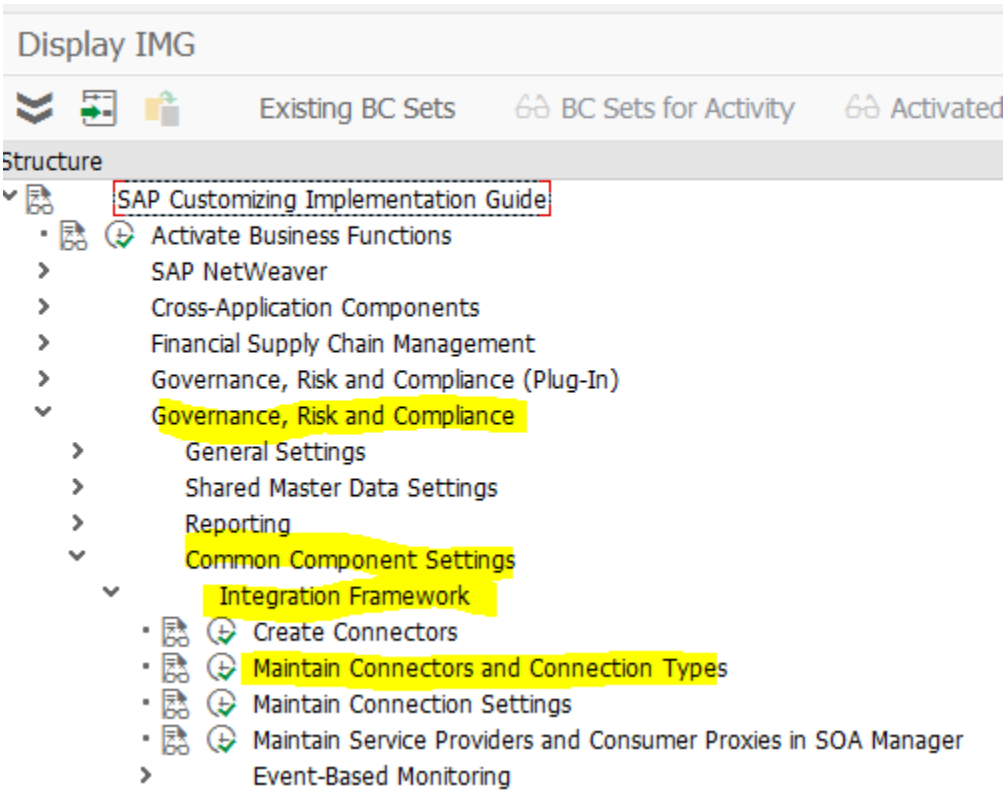
4) Creating and Maintaining connectors.

- Establishing RFC Connections.
- **Please listen again**

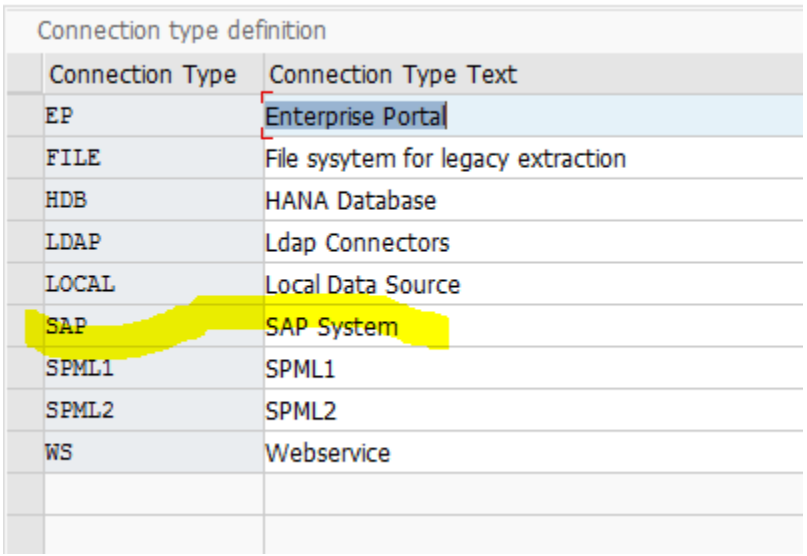
5) Maintaining Connectors and connection types.

Purpose of Connectors is to fetch the data from Backend to GRC

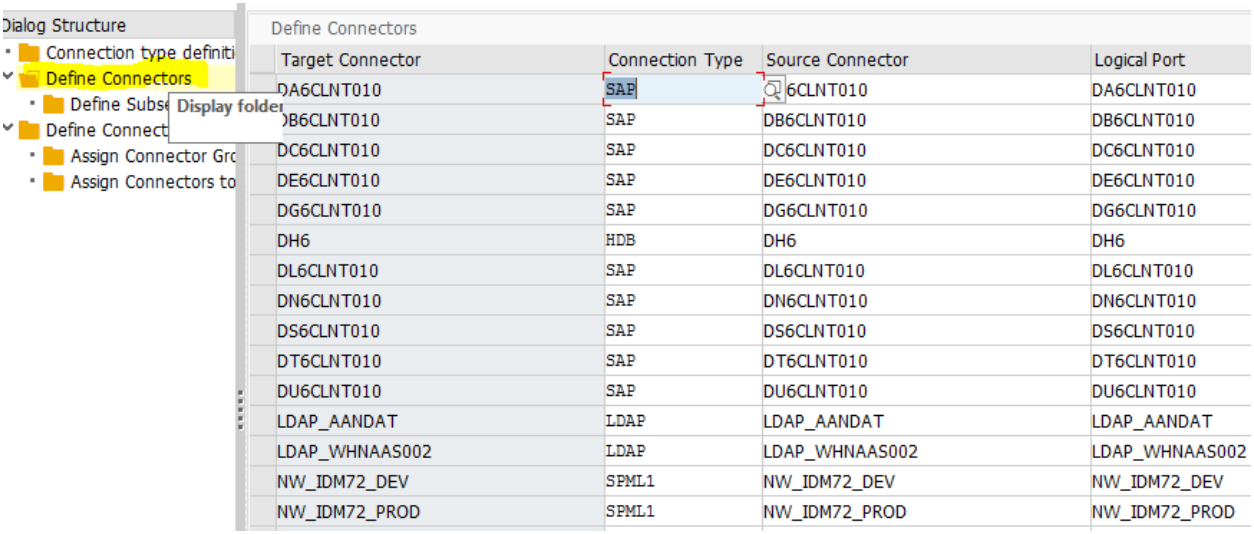
GRC-SPRO-SAP Reference IMG GRC…..> Common Component Settings-- Integration Frame work---- Maintaining Connectors and connection types.



Select Connection type SAP



Double click on “ Define Conectors” and “ New Entries” add details.



Target Connector: ECCCLNT010

Connection Type: SAP

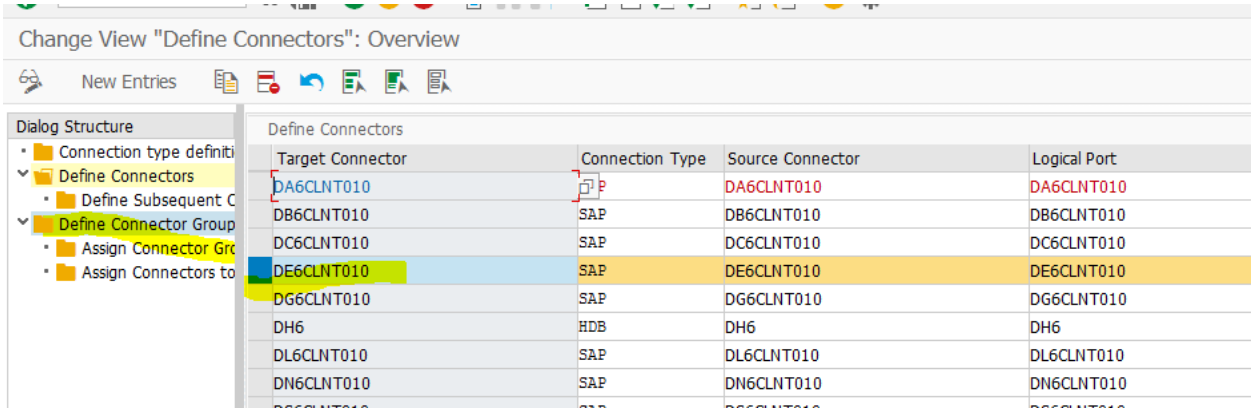
Source Connector: ECCCLNT010

Logical Port: ECCCLNT5010

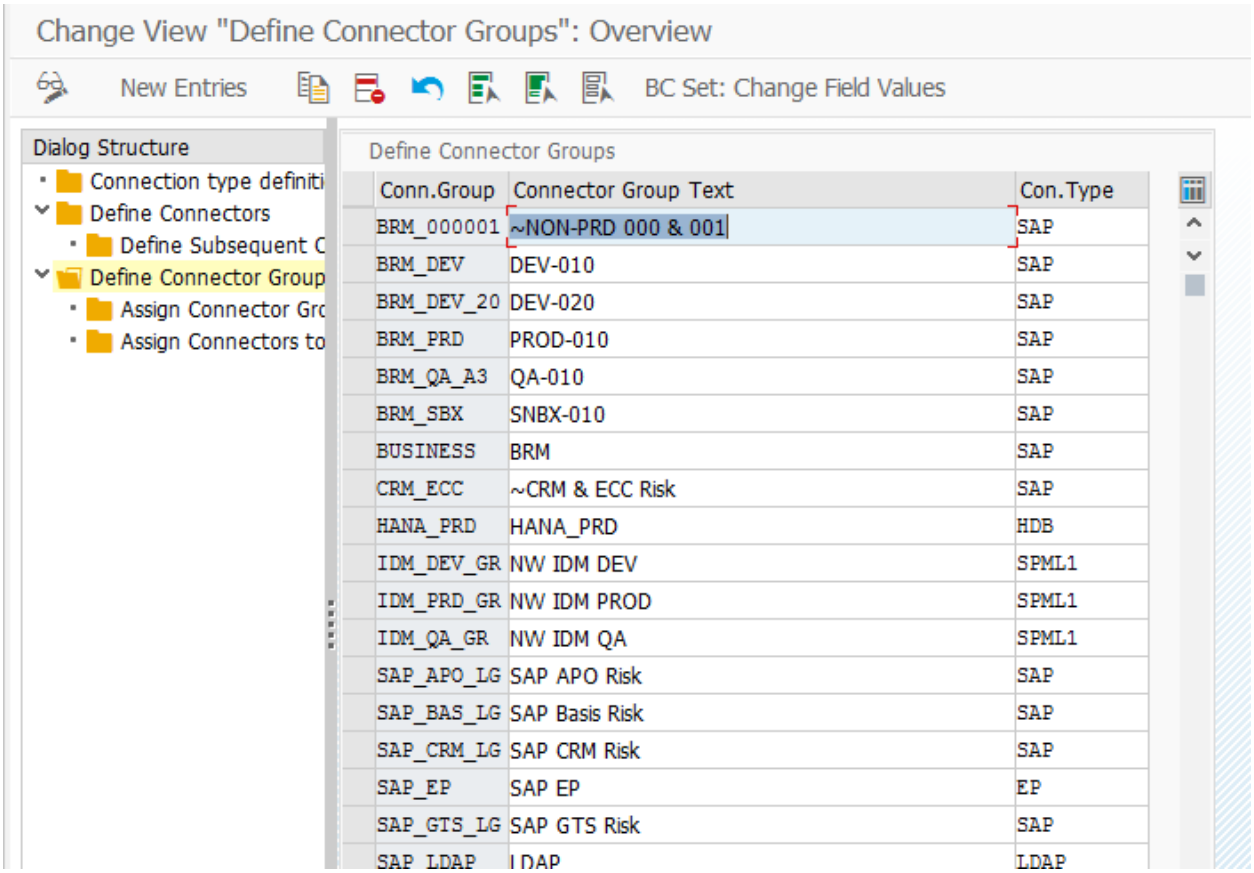
Max no of BG WP: 3

And save.

Now, select connector and double click on “ Define Connector Groups”



We can use existing /create new one (“New Entries”)



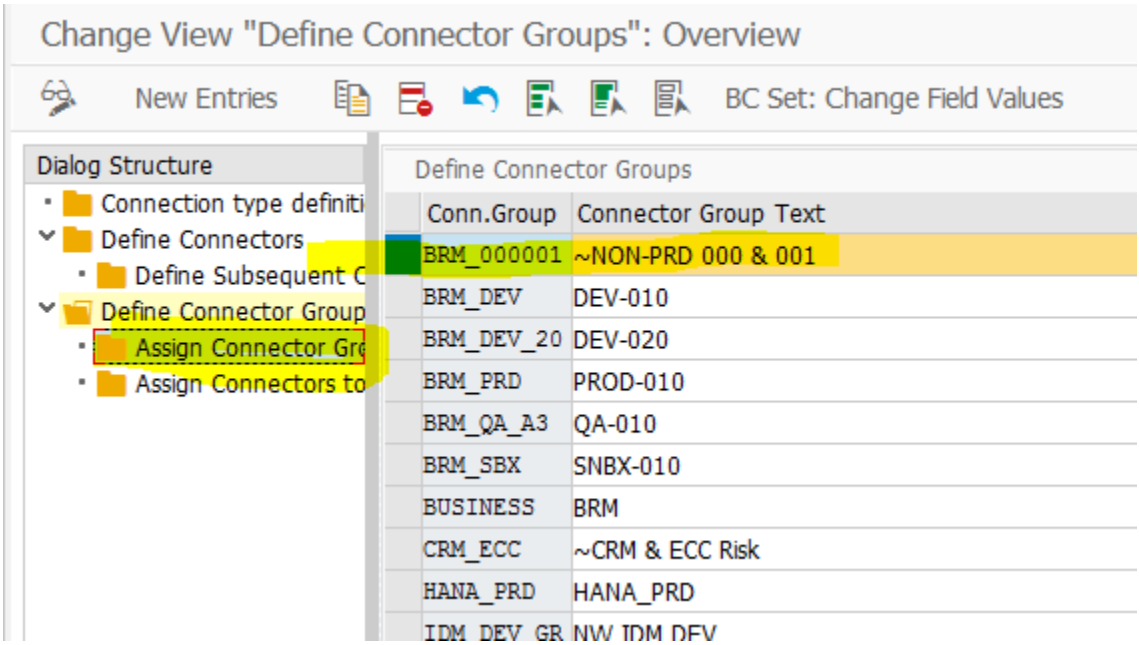
The reason why we use connector group is …If we have only 1 GRC system(1 system Landscape….generally..it will not be there in LIVE Environment)..it gets connected to Ecc Dev , Ecc Prod.

We will define connector group as Ecc in which we have Dev, Qua, Prod

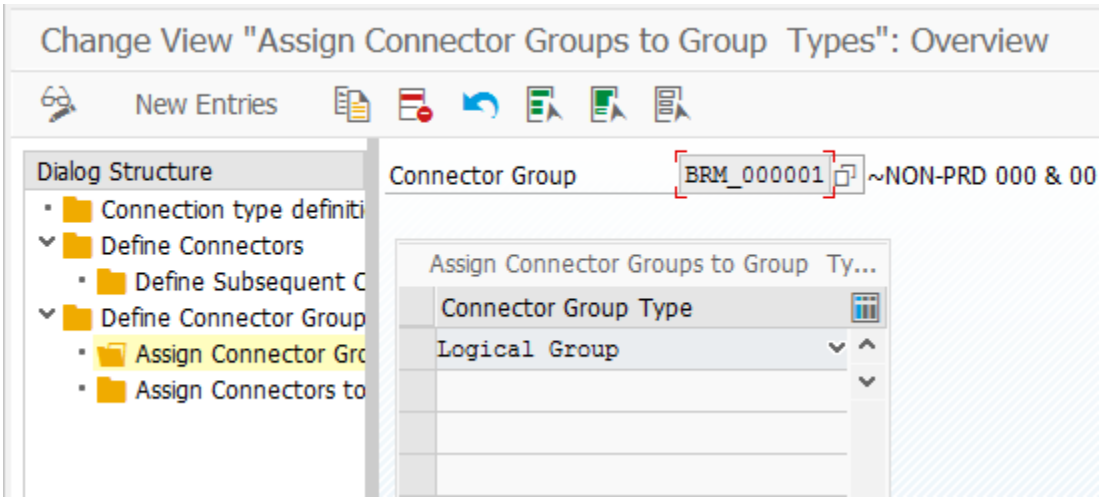
Connector group: Group systems to one group.

Now, we need to define Connector group and what is this connector group?

Double click on “ Assign Connector Group to Group Types”



Its logical group

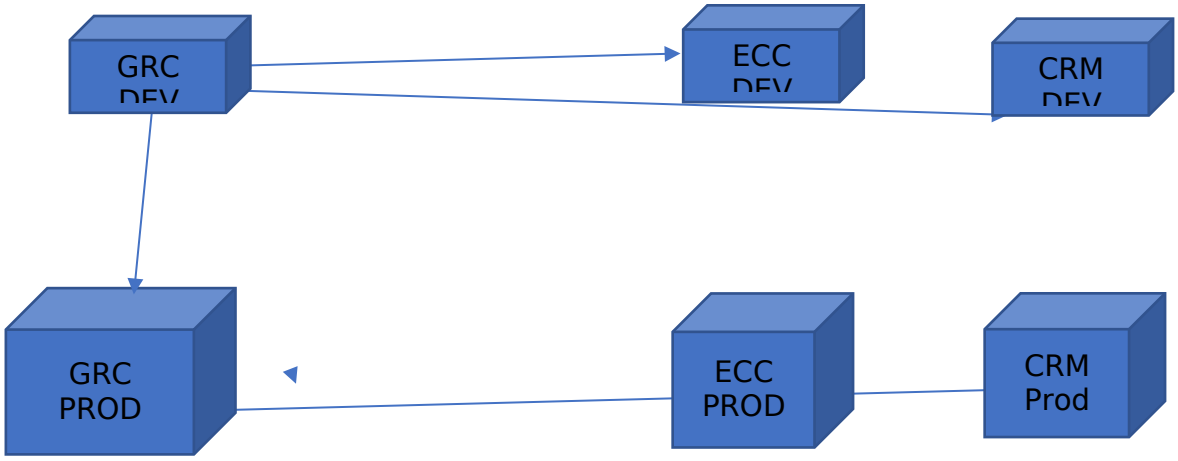


Now select this “Logical Group” click on “ Assign Connectors to Connector groups” New entries”

Now , what ever we define in “ Define Connectors”, those will be available.

GRC Landscape:

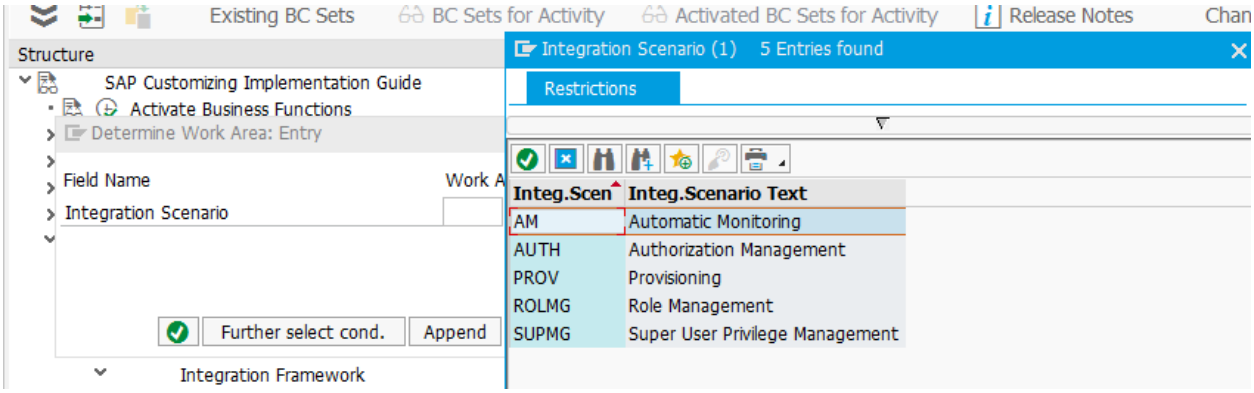
- It depends on company to company whether they implement 3 system land scape **or** 2 system land scape
- 1 system is Dev and Quality and other is for Prod.(2 system land scape)
- As GRC is technical system, we can have 2 system land scape . where as ECC is Business system, we need to have 3 system landscape.



- GRC Dev Communicates with ECC Dev, CRM Dev
- GRC Prod Communicates with ECC Prod, CRM prod
- GRC brings the data like users and roles from Backend systems like ECC, CRM
- **GRC Dev to GRC Prod: Customized objects/Configuration we do in GRC DEV (Whatever we develop) will moved to GRC Prod.**
- We bring users and roles to GRC Dev from ECC Dev. But , this data will not be moved to GRC Prod.
- Data like users and roles will not be moved to GRC prod from GRC dev.
- So, only customized object will move not data.
- No concept of Transport to bring data from Ecc to GRC. We have only Import concept.
- GRC is a technical system and it provides services to multiple Landscapes.

Maintain Connection Settings: (Interview Question & Certificate Question)

- GRC-SPRO-SAP Reference IMG GRC.....> Common Component Settings-- Integration Frame work----Maintain Connection Settings.



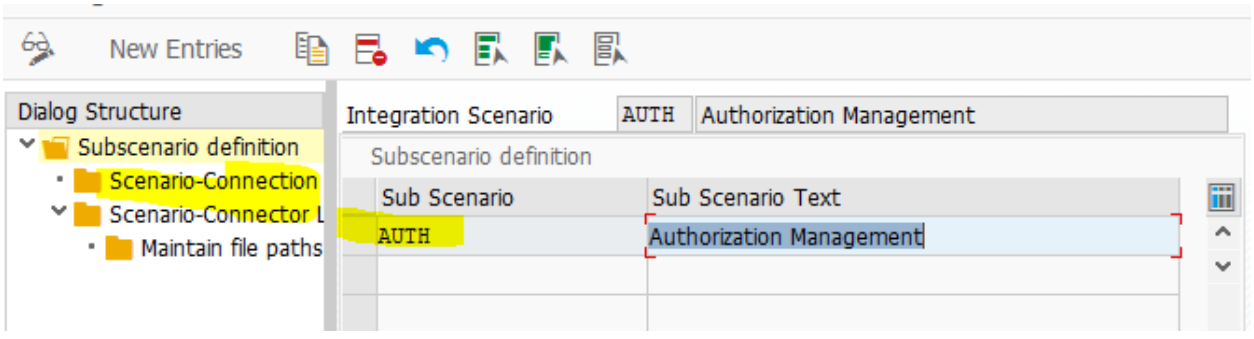
AUTH is the integration scenario for ARA

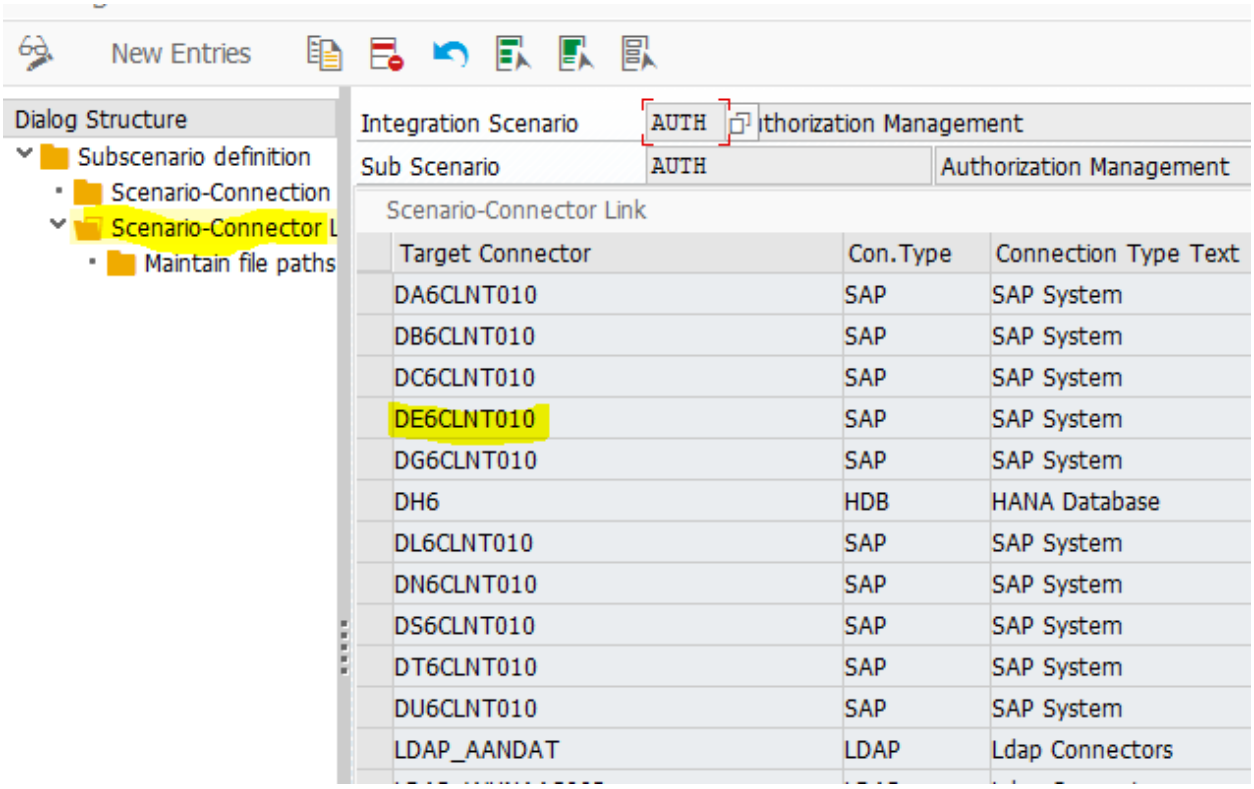
PROV is the integration scenario for ARM

ROLMG is integration scenario for BRM

SUPMG is the integration scenario for EAM

1) Select “AUTH” and ok.
2) Select “ Scenario connection Type link” and select SAP and select SAP and click on “Scenario Connector link”





- What these step mean…ARA(AUTH) is activated for This connector(DE6CLNT010)
- It means ARA component work/implemented for this Connector.
- If we don’t define “AUTH” for this connector(DE6CLNT010), you can not use ARA for this system.
- Means data will not fetched GRC from Backend.
- We can not perform Risk Analysis, we can not fetch data from Source/Backend system.
- Whatever operations we perform using ARA ,will not work.
- Connector should understand what component(ARA,ARM, BRM, EAM) is integrated with it.

Same steps for PROV, ROLMG, SUPMG

GRC Roles

1) We have almost 28/29 GRAC roles
2) By default, these roles are not generated. We need to generate with SUPC.

3) Copy standard role to custom role and assign to users.

- **SAP_GRAC_ACCESS_APPROVER**: Each approver, it can be role approver/Mitigation approver/Risk approver who approves the request should have this role.
- **SAP_GRAC_ACCESS_REQUEST_ADMIN:** user who is administrating all access requests should have this role.
- **SAP_GRAC_ACCESS_REQUESTER:** All end users need to have this role to request Access Request. (If they want new role/any changes required in User id) . To request these, user should have this role.
- **SAP_GRAC_ALERTS:** We can configure SOD Alerts
- **SAP_GRAC_ALL:** Its like SAP_ALL . All access to AC Application
- SAP_GRAC_ACCESS_REQUESTER, SAP_GRAC_END_USER, SAP_GRAC_NWBC, SAP_GRAC_BASE Should be assigned to all users. We can say Common roles for all users.
- **SAP_GRAC_CONTROL_APPROVER:** The content of mitigation needs to be approved by Mitigation Control approver. SO, this role will be assigned to Mitigation control approver.
- **SAP_GRAC_CONTROL_MONITOR:** If we mitigate any user, there should be someone to monitor this user.
- **SAP_GRAC_CONTROL_OWNER:** Each and every Mitigation control you create in the system, should be approved by Mitigation control owner.
- For every mitigation control id, there will be one mitigation control owner who is responsible to assign mitigation control id to user.
- For ex, If I want to mitigate a user, I need to assign mitigation id to user. Then request goes to Owner and t it has to be approved by owner. Then only user mitigated.
- **SAP_GRAC_DISPLAY_ALL:** All the access but only display.
- **SAP_GRAC_FUNCTION_APPROVER:** What ever function you create in system, The content of function needs to be approved be function approver.
- **SAP_GRAC_REPORTS:** User who has access this can perform auditing activities.
  We can run all AC reports
- **SAP_GRAC_RISK_ANALYSIS:** User can Risk Analysis if its assigned.
- **SAP_GRAC_RISK_OWNER:** For each risk you create in the system, there must be Risk Owner who is responsible to approve the content of risk.

- **SAP_GRAC_RULE_SETUP:** We can create Rule set with this.
- **SAP_GRAC_SETUP:** We can perform setup activities in AC.

BRM related roles:

- SAP_GRAC_ROLE_MGMT_ADMIN
- SAP_GRAC_ROLE_MGMT_DESIGNER
- SAP_GRAC_ROLE_MGMT_DESINGER
- SAP_GRAC_ROLE_MGMT_ROLE_OWNER
- SAP_GRAC_ROLE_MGMT_USER

EAM Role:

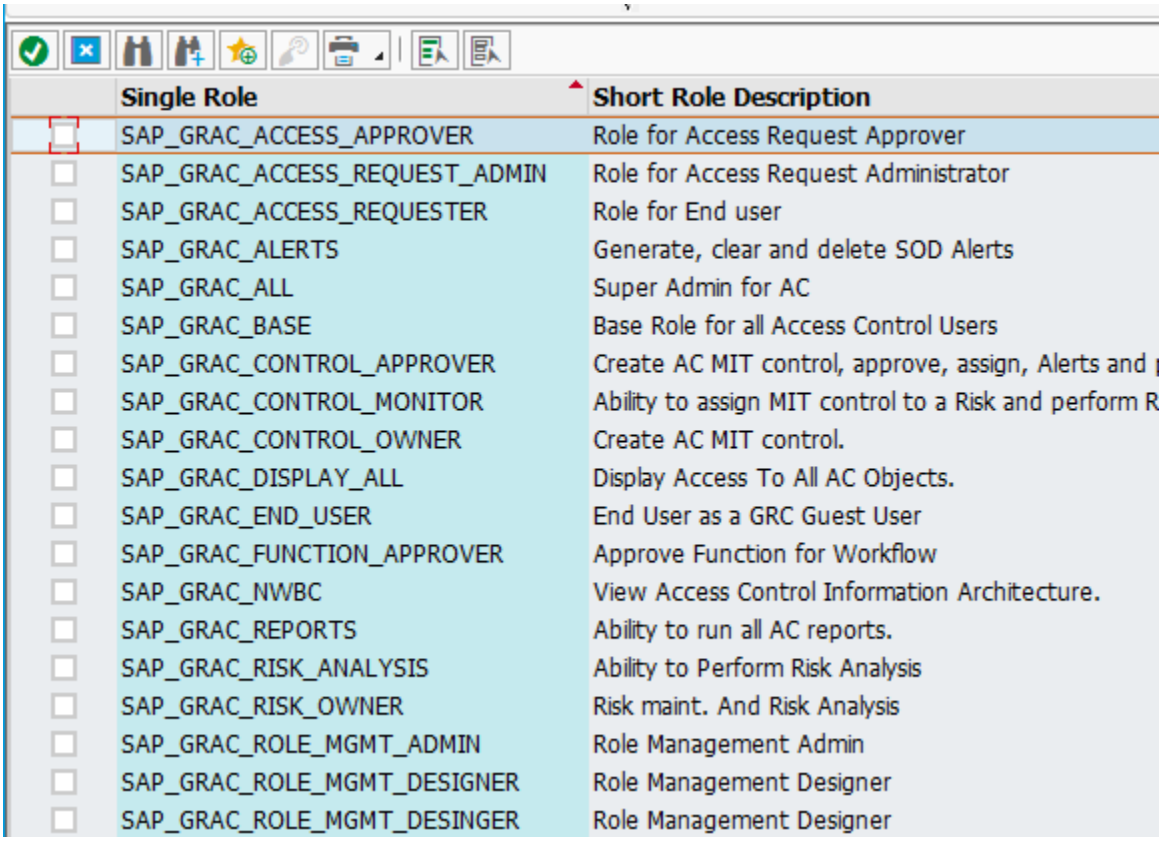
SAP_GRAC_SPM_FFID

SAP_GRAC_SUPER_USER_MGMT_ADMIN

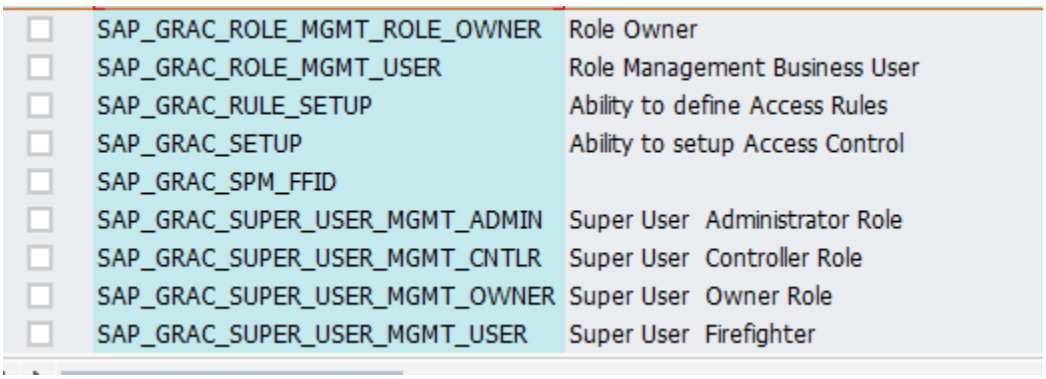
SAP_GRAC_SUPER_USER_MGMT_CNTLR

SAP_GRAC_SUPER_USER_MGMT_OWNER

SAP_GRAC_SUPER_USER_MGMT_USER



Single Role	Short Role Description
SAP_GRAC_ACCESS_APPROVER	Role for Access Request Approver
SAP_GRAC_ACCESS_REQUEST_ADMIN	Role for Access Request Administrator
SAP_GRAC_ACCESS_REQUESTER	Role for End user
SAP_GRAC_ALERTS	Generate, clear and delete SOD Alerts
SAP_GRAC_ALL	Super Admin for AC
SAP_GRAC_BASE	Base Role for all Access Control Users
SAP_GRAC_CONTROL_APPROVER	Create AC MIT control, approve, assign, Alerts and
SAP_GRAC_CONTROL_MONITOR	Ability to assign MIT control to a Risk and perform R
SAP_GRAC_CONTROL_OWNER	Create AC MIT control.
SAP_GRAC_DISPLAY_ALL	Display Access To All AC Objects.
SAP_GRAC_END_USER	End User as a GRC Guest User
SAP_GRAC_FUNCTION_APPROVER	Approve Function for Workflow
SAP_GRAC_NWBC	View Access Control Information Architecture.
SAP_GRAC_REPORTS	Ability to run all AC reports.
SAP_GRAC_RISK_ANALYSIS	Ability to Perform Risk Analysis
SAP_GRAC_RISK_OWNER	Risk maint. And Risk Analysis
SAP_GRAC_ROLE_MGMT_ADMIN	Role Management Admin
SAP_GRAC_ROLE_MGMT_DESIGNER	Role Management Designer
SAP_GRAC_ROLE_MGMT_DESINGER	Role Management Designer



SAP_GRAC_ROLE_MGMT_ROLE_OWNER	Role Owner
SAP_GRAC_ROLE_MGMT_USER	Role Management Business User
SAP_GRAC_RULE_SETUP	Ability to define Access Rules
SAP_GRAC_SETUP	Ability to setup Access Control
SAP_GRAC_SPM_FFID	
SAP_GRAC_SUPER_USER_MGMT_ADMIN	Super User Administrator Role
SAP_GRAC_SUPER_USER_MGMT_CNTLR	Super User Controller Role
SAP_GRAC_SUPER_USER_MGMT_OWNER	Super User Owner Role
SAP_GRAC_SUPER_USER_MGMT_USER	Super User Firefighter

Maintain Configuration Settings

- Via RZ10 T-code, we maintain parameters. Same way, for AC parameters will be configured here.

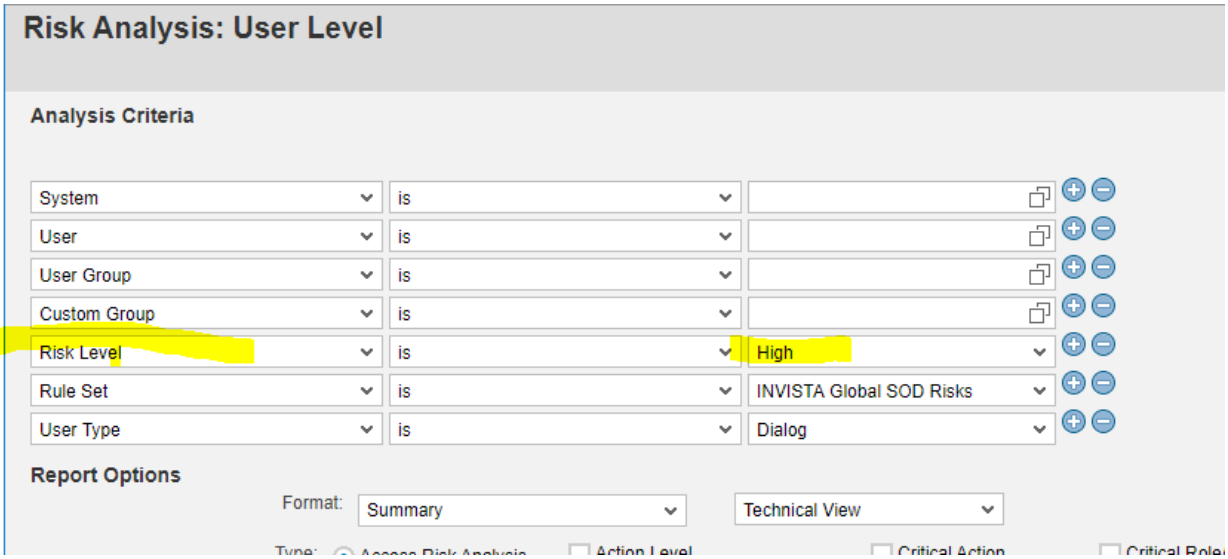
- We are going to perform all activities/functionalities of AC via NWBC and it opens in web browser. (NetWeaver Business Client)
- My home, Setup, Access Management, Reports and analytics are called “Work Centers”
- **My home:** is common work center for all users
- **Setup**: we can perform configurations steps
- **Access Management:** We can perform support and maintenance activities.
- **Reports/Analytics:** We can perform reporting activities. Its for Auditing purpose.

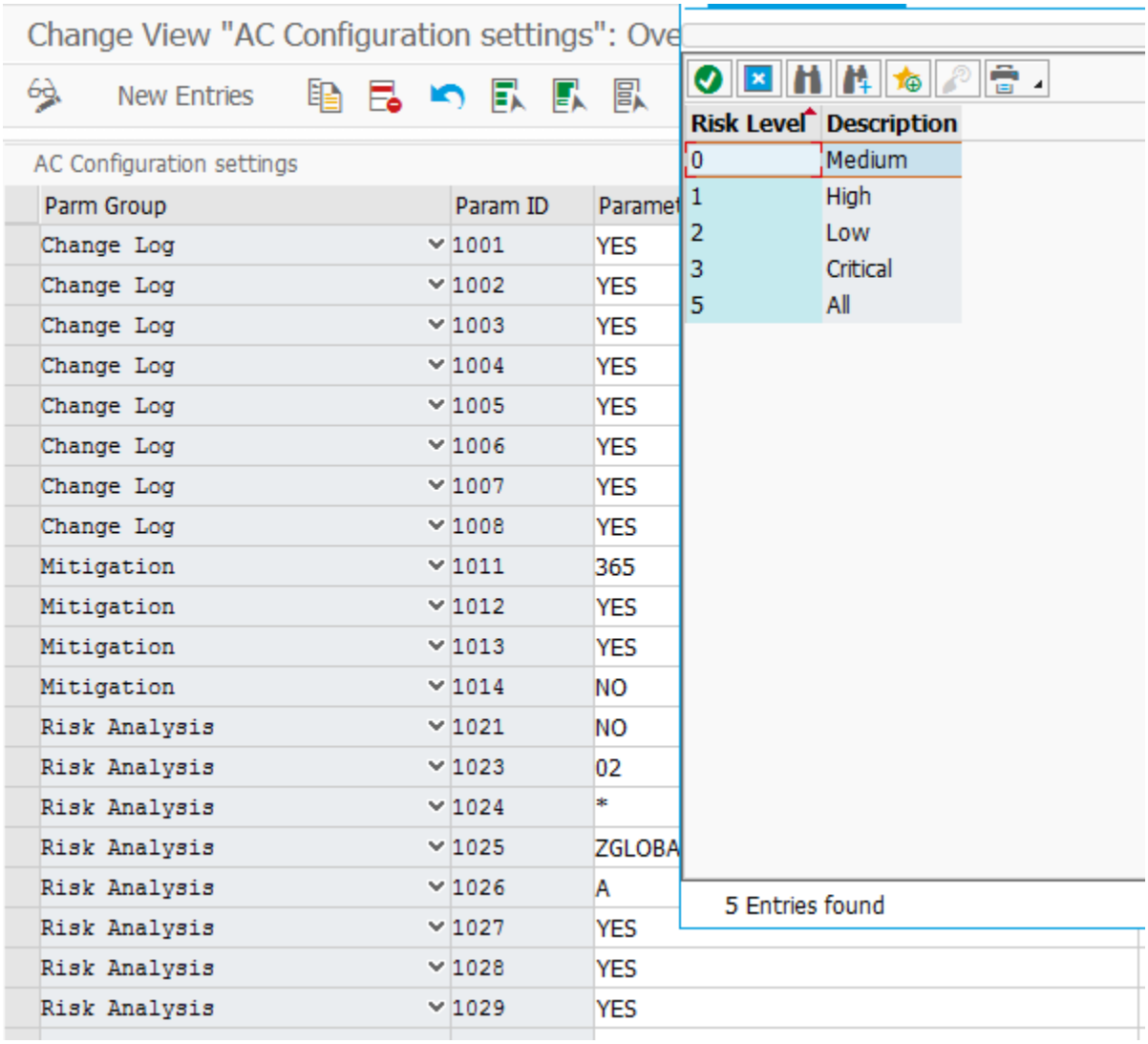
Note: Depends on the role assigned to user, user will get access to functionalities of this WorkCentre.

When we go to risk analysis at user level, we can see default value as “ HIGH” at Risk level option. This can be set in below path. (Who will ask us to maintain “HIGH” .....Business or ourself)???????????????

Based on our requirement, we can set any value.

GRC---SPRO—SAP Reference IMG----GRC----AC----Maintain Configuration Settings





- All Risk Analysis parameters will be available in " Risk Analysis" Parameter group.
- GRACCONFIG is a table where we can find default vaues

AC Configuration settings

Parm Group	Param ID	Parameter Value	Priority	Description
Risk Analysis	1024	*	0	Default risk level for risk analysis
Risk Analysis	1025	ZGLOBAL	0	Default rule set for risk analysis
Risk Analysis	1026	A	0	Default user type for risk analysis
Risk Analysis	1027	YES	0	Enable Offline Risk Analysis
Risk Analysis	1028	YES	0	Include Expired Users
Risk Analysis	1029	YES	0	Include Locked Users
Risk Analysis	1030	YES	0	Include Mitigated Risks
Risk Analysis	1031	YES	0	Ignore Critical Roles & Profiles
Risk Analysis	1032	YES	0	Include Reference user when doing user analysis
Risk Analysis	1033	YES	0	Include Role/Profile Mitigating Controls in Risk Analysis
Risk Analysis	1034	100	0	Max number of objects in a package for parallel processing
Risk Analysis	1035	YES	0	Send email notification to the monitor of the updated mitig
Risk Analysis	1036	NO	0	Show All Objects in Risk Analysis

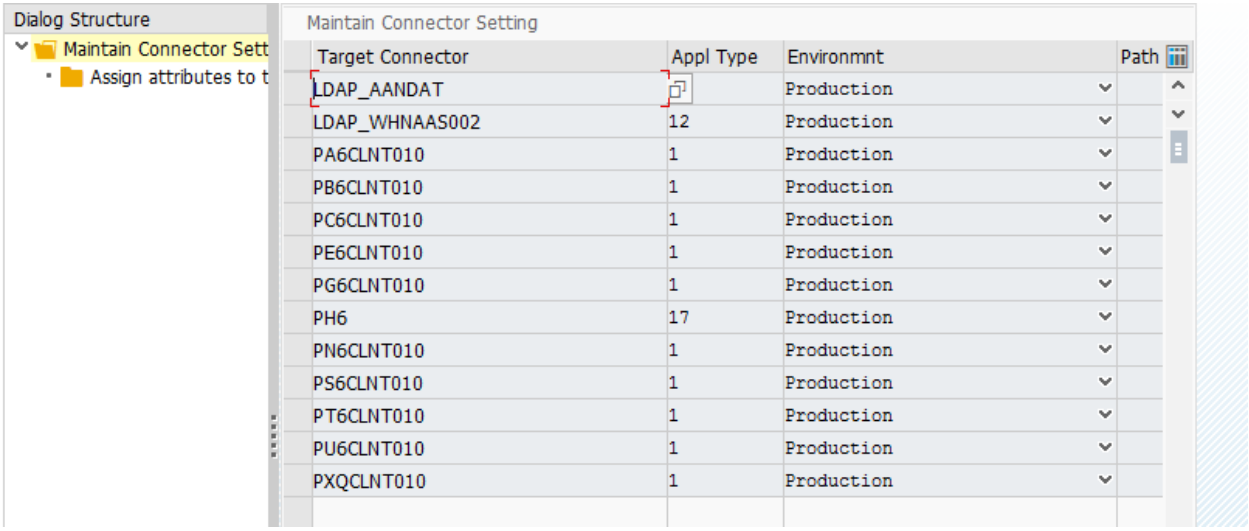
ARA parameters starts with 10
ARM parameters starts with 20
BRM parameters starts with 30
EAM parameters starts with 40
We have almost 191 parameters available in GRC10.1

- C

8) Maintain Connector Settings

- **This is very simple steps.**
- **Here we are going to define " Environment". Whether Backend system is Dev or Qua or Prod.**

Path: GRC---SPRO—SAP Reference IMG----GRC----AC----Maintain Connector Settings



9) Maintain Mapping for Actions and Connector Groups

- This is one of the most imp configuration step.
- GRC---SPRO—SAP Reference IMG----GRC----AC---- Maintain Mapping for Actions and Connector Groups
- This step is for BRM Component
- GRC---SPRO—SAP Reference IMG----GRC----AC---- Maintain Mapping for Actions and Connector Groups----" New Entries"

- Connector Group: ECCCONNECTOR
- Active Check box
- App Type: SAP
- Save
- Now, select this connector group and” assign default connector to Connector Group”
- New Entries
- Connector Group
- Actions:
- Target Connector:
- Default: Check Box

We can maintain roles in below path.(Creation)

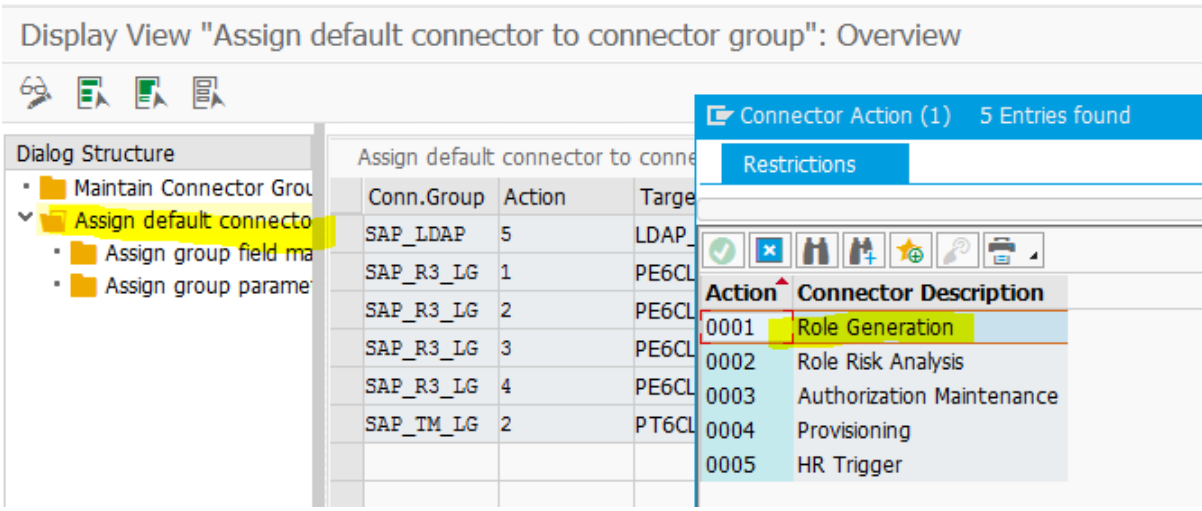
Role Maintenance—Create---Single Role

In This screen , we can see below path/Stages.

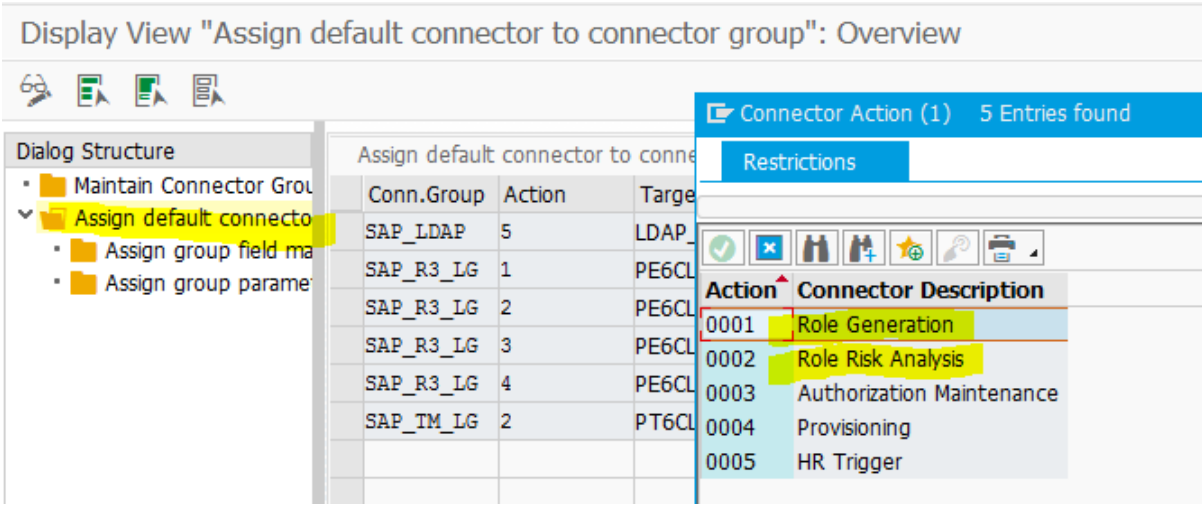
When we try to create , there are many below stages.

Define Role---Maintain Authorizations---Analyse Access Risk----Derived Role-----Request Approval-----Generate Roles------Maintain Test Cases.

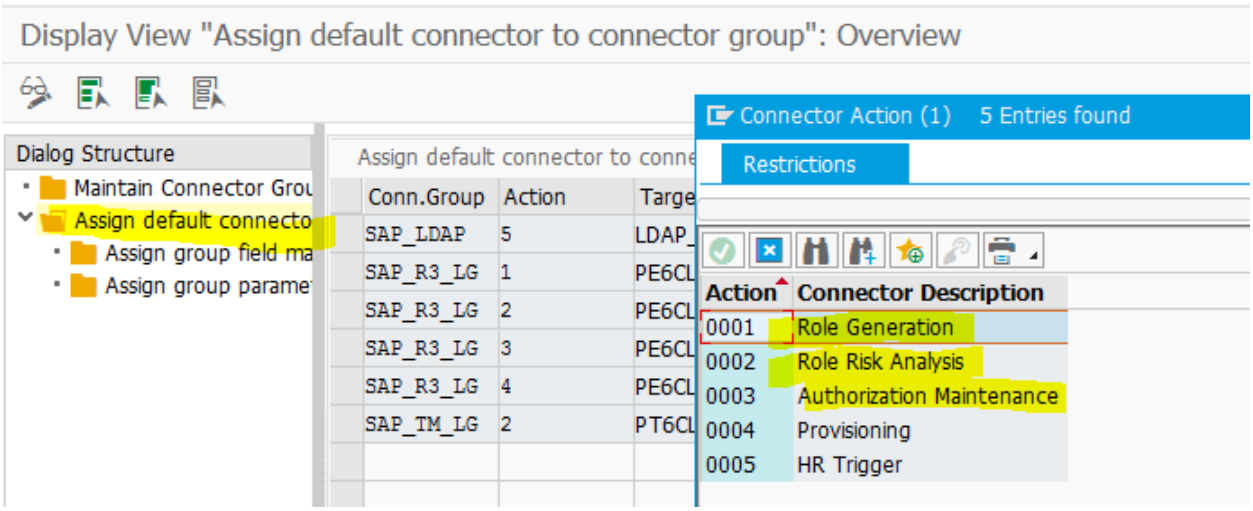
- If you want to generate role, you need maintain this in action in below path.
- If you don’t maintain 0001, you cannot generate role in BRM while creating role.



- We need to maintain 0002 in action to perform risk analysis.
- If we don’t maintain 0002 in Actions, we can not perform risk analysis.



- To maintain T-codes/Objects, 0003 should be maintained in “ Action”
- If we don’t maintain, you can not add T-codes.



- The role created in BRM has to be provisioned to Backend system. For this we need define 0004 in " Actions: Else, we can not provision to Backend system

10) Maintain Plugin Settings

- This is the only step we need to perform in Backend system
- Login to Backend system(Ecc)
- SPRO----SAP Reference IMG----GRC (Plug in)—AC----Maintain Plugin Configuration Settingse
- New Entries
- Parameter Id : 1000 (Maintain Plugin Connector)
- Sequence : 1
- Parameter Value: ECCCLNT010
- Save.
- New Entries
- Parameter Id : 1001 (Maintain GRC Connector)
- Sequence : 2
- Parameter Value: GRCCLNT010
- save
- We maintained 2 parameters 1000 and 1001
- Which means we are informing system that ECCCLNT010 is your connector and you to respond to GRCCLNT010 system.

11) Synchronization Jobs

- GRC---SPRO—SAP Reference IMG----GRC----AC---Synchronization Jobs----Auth Synch
- **Auth Synch:**
- In Su24, we maintain Auth Objects, Auth Obj check indicators and Auth obj values
- This data Will be stored in USOBT_C and USOBT_X
- GRC System should the know the Security structure which means T-codes and Its Auth Objects.
- Based on this GRC system will perform risk analysis
- This data we bring it from ECC to GRC
- GRC---SPRO—SAP Reference IMG----GRC----AC---Synchronization Jobs----Auth Synch
- Select Connector---Program----Execute in Background.—Immidiate---Check---Save
- Background Job (GRAC_PFCG_AUTHORIZATION_SYNC) which brings Su24 data to GRC from ECC.
- **Repository Object Synch:** We are going to bring role, profiles and users to GRC from ECC
- Select the Connector, If we are doing this 1st time, always select " Full Synch Mode"
- You have already 100 user 10 roles . Now you create 20 more users and 5 more roles. To bring these newly created data ..select " Incremental Synch Mode"

Interview Question:

GRACUSERCONN is table in GRC to find all users
GRACRLCONN is a GRC table to find all roles

12)

Generating Rule Set

- Rule set is logical container which consists of Risk, Function, Business Process.
- Function: is part of Rule set and Contains actions(T-code) and Permissions (Auth Object)

- I am creating one function(FUNCTION 1) with Su01, Su10, SUGR---User Admin T-codes
- Creating one more function (FUNCTION 2) with PFCG, SUPC----Role Administration T-codes
- SOD: Segregation of Duties
- SOD says one individual should not have complete control over a process or should not have conflict Auth/Permission
- For ex: One user " UPPALAVE" has Su01 (Function 1) and PFCG (Function 2)
- Combination of multiple Functions gives SOD Risk.
- Now, We defining FUNCTION 1, FUNCTION 2 as Risk Z_RISK
- It means, user who gets access to combination of Function T-codes will get Risk (Z_RISK)
- We are defining the risk/We are informing the system.
- **Su01, Pfcg- Risk,**
- **Su10, Pfcg-Risk**
- **SUGR, Pfcg- Risk**
- **Su01, SUPC- Risk**
- **Su10, SUPC-Risk**
- **SUGR, SUPC- Risk**
- We can define multiple functions under one Risk

Function 1:	Function 2:	Function 3:
Su01, Su10, SUGR	Pfcg, SUPC	SM30, SE16N,SE38,STMS

Any combination of different function T-codes gives a risk.

Business Process: This Risk belongs to which Business process; we need to define.

This Risk Belongs to "Basis "Business Process.

Note: Complete GRC is based on this Rule set Architecture

Note: Standard rule set given by SAP is called "GLOBAL RULESET"

So, we need to create Customize Rule set, Customize Functions, Customize Risk, Customize Business process though SAP has given Standard one as we may not use standard one like we don't user standard Roles

- We need to activate content of Global Rule Set.

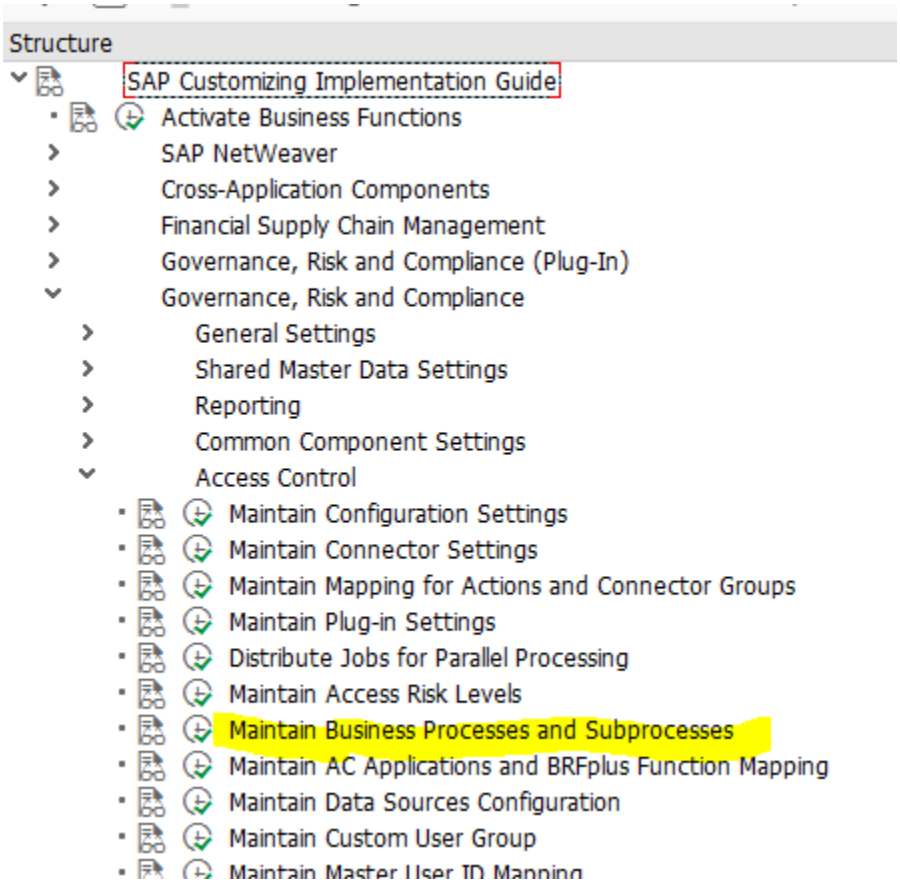
- GRC---SPRO—SAP Reference IMG----GRC----AC---Access Risk Analysis----SOD Rules----Generate SOD Rules. Select “*” and execute. Now, All Risks will be generated. (It takes some time)
- Now we can see the list of All Risks.
- We need to generate all standard Risk to perform Risk Analysis. Not only Standard Risk, Any risk we create we need to generate before we use for Risk Analysis.
- We can check the all these in NWBC..” SETUP”….

ARA

- We are going to create Customized Ruleset, Customized Risks, Customized Functions, Customized Business Process.

How to create Customized Business Process:

- GRC----SPRO---- SAP Reference IMG--▯ GRC-----Access Control----Maintain Business Processes and Sub Processes----New Entries---Give required BP name and description and save and it ask for TR.
- Select newly created BP and click on “ Business Subprocess” and New Entries and enter Subprocess and description and save.
- Ex: Business Process: Finance
- Sub Business Process: Accounts Payable, Accounts Receivable, GL



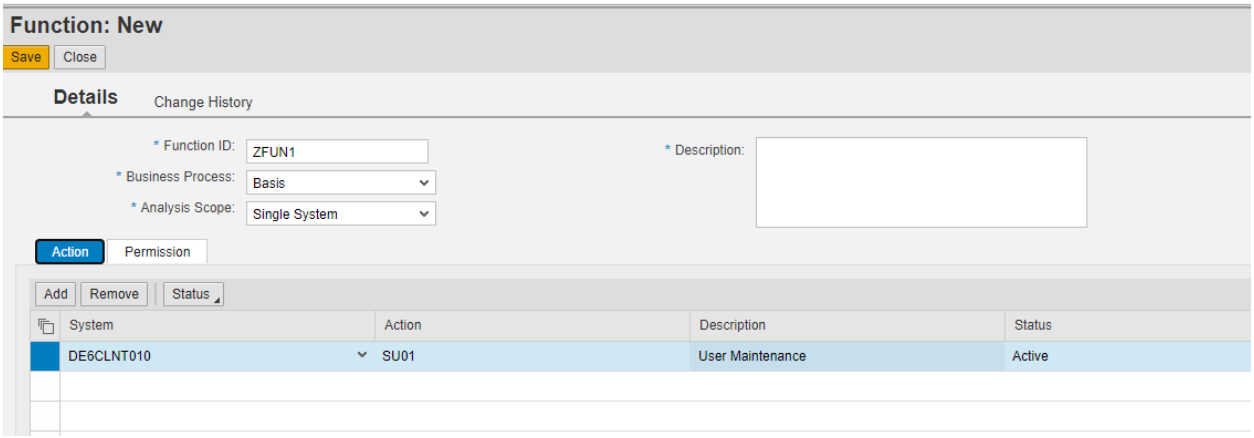
How to create Customized Rule Set

- We can create this in NWBC
- GRC---NWBC---Setup—Access Rule Maintenance---Rule Set—Create and given name and save.
- We cannot see any data/Content in it. Its just a logical Container

How to create Customized Functions

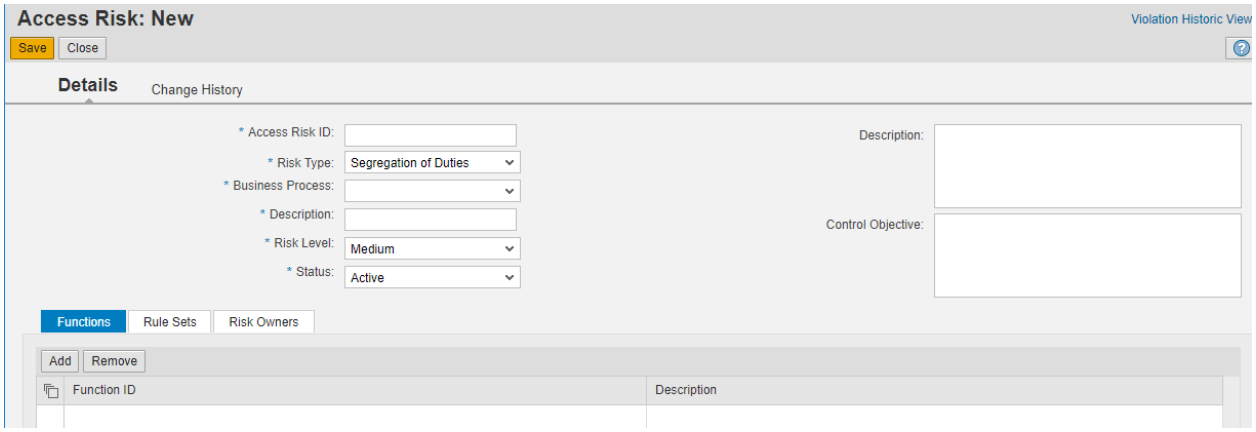
- GRC---NWBC---Setup—Access Rule Maintenance—Functions---Create
- Fill below required fields.
- Function Id(ZFUN1), Business Process,Description,analysis scope
- Add---System, Action.

- We can add multiple Actions(T-codes) in one Functions based on requirement.
- Go to “Permissions”…Su01 relevant object will be shown.
- By Default, all permissions will be “ Inactive”.
- There are few Auth Objects which are very critical for SU01.
- S_USER_PRO is critical Auth Object and activity 22.
- Through which we can assign Profiles like SAP_ALL can be given to users/Own. So, its risk
- So make it as “ Active”
- Save the function(ZFUN1)
- Now, create a another function ZFUN2 and follow same steps.
- ADD---Action—PFCG..
- Go to” Permissions”..PFCG relavant Auth Objects will be shown.
- S_USER_AGR (Actvt 22)is critical Object. We can assign Roles to users. Make this as active and save.



Now, we are creating Customized Risk.

- GRC---NWBC---Setup—Access Rule Maintenance---Access Risks----Create
- Risk id should be created and generated.
- Fill in all required fields.
- Access Risk Id: BASRISK
-
-



Interview Question and Certification Question.

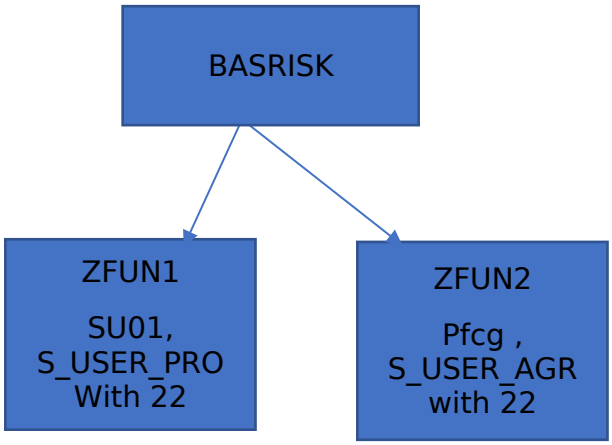
How many type of risk we have.

Ans 3:

SOD

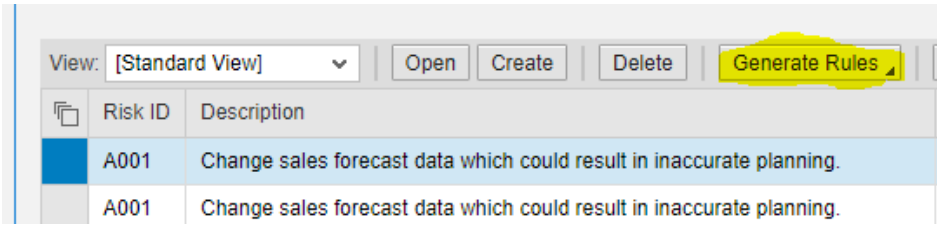
Critical Action

Critical Permission



- Go to “ADD”----Functions---Add functions---“Ruleset”…given Ruleset name
- Risk Owner: For each and every Risk, there must be “Risk Owner” who is responsible to approve this Risk.
- Create a user “Riskowner” via su01 in GRC and assign required roles for risk owner(3 Basic Roles and SAP_GRAC_RISK_OWNER)
- We have to maintain this user in “Access Control Owners”
- Setup----Access control Owners

- Create and give required details and save.
- Now this user is a “ Risk Owner”
- Now we need to generate the Risk. (With out generating risk, we can not user this risk when performing Risk Analysis.
- GRC---NWBC---Setup—Access Rule Maintenance---Access Risks---Select risk---generate Rules

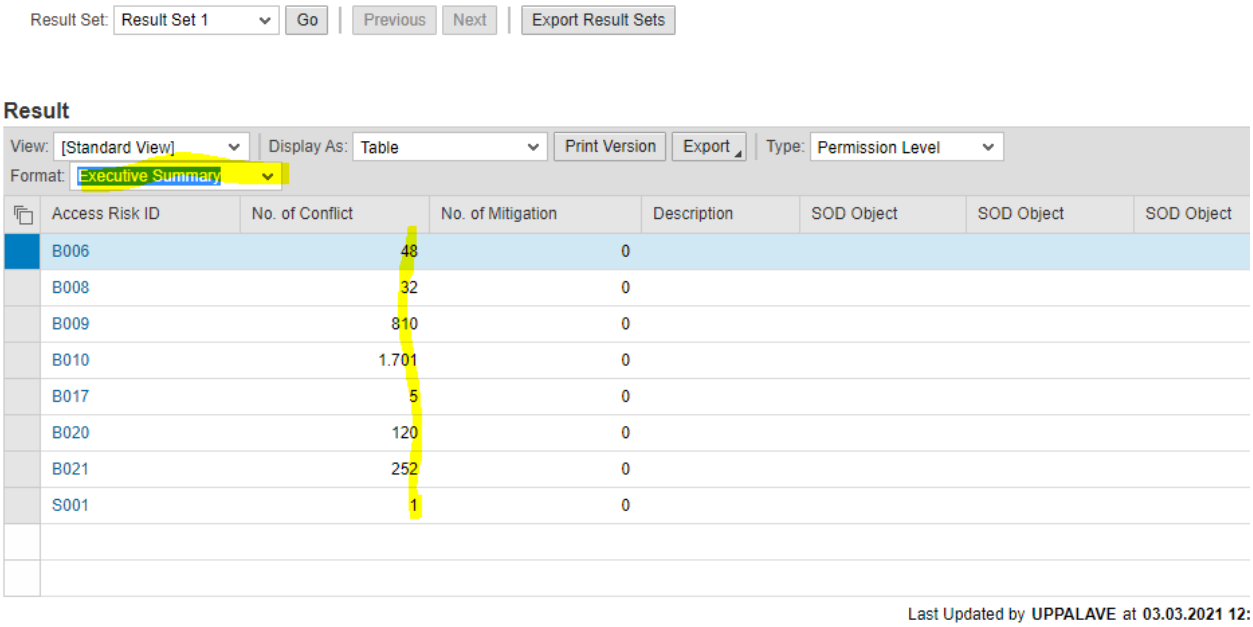


Note: Risk owner id should have SAP_GRAC_RISK OWNER role+3 Basic roles and should be maintained in “ Access Control Owners”

- Now, we have to run Risks analysis.
- If we try to assign su01 and pfcg, we should get Risk(BASRISK)
- In Backend system , create 2 roles with su01 and pfcg
- Role ZTEST1 with su01, pfcg and S_USER_PRO with 22, S_USER_AGR with 22
- Role ZTEST2 with SM36, SM37

- Add these roles to 2 users User1, User 2respectively.
- Get these users and roles to GRC.
- GRC---SPRO—SAP Reference IMG----GRC----AC---Synchronization Jobs----Repository Object Synch—"Incremental Synch”(Only newly created will be moved to grc)
- Now run “Risk Analysis” at user level for user1 who has su01, pfcg
- User will get BASRISK
- Su01, pfcg will give action level risk. S_AGR_USER with 22, S_USER_PRO with 22 will get Permission level risk.
- Format: Summary, Detail, management Summary, Executive Summary
- Executive Summary: It will show Risk Id, no of Conflicts
- If No of conflicts shows 1(su01, pfcg), if we remove one of them, user will be risk free
- When you run Risk analysis for user, we don’t get any risk. Because, we did not define the risk for SM36 and SM37

Below is the example of “Basis role” risk analysis (Role Level)



Note1: Once you get risk analysis report, by default it shows risk at” Action Level” and format is Summary. If you want permission level risk report, Change it to Details from Summary in Format.

Note 2: We can run risks analysis in the background also when we have large data.

Advantage is it will be stored/saved/available. When perform in “Foreground and close it, we have to run again if you want.

This functions and Risks, T-codes and Permissions will be given by Basis Team.

We are not deciders to define what is risk

It is define by Business team, Technically we do it in system.

Based on this, we have to build Ruleset.

When we found risk, We do 2 activities

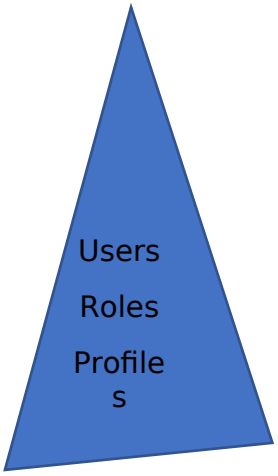
Remediation&Mitigation

1) **Remediation**: Removing the risk from user/Role/Profile is called Remediation
2) For ex there is a role which has risk and assigned to 1000 users , now these 1000 users will get risk. Root cause of risk is Role.
3) Remediation is nothing but making user risk free
4) If you don’t want risk at “Action Level”…then go for T-code removal.
5) If you don’t want risk at “Permission Level”..Then go for Activity removal
6) There is big process for Remediation
7) **Mitigation: Allowing the risk** to user/role/profile is called Mitigation
    - Based on company requirement, sometimes we need to allow the risk.
    - So, there should be some person who monitor his/her activities
8) When we mitigate risk at Role level, no users will get Risk who has this role.

Hierarchy of the Risk

1) Risk comes to user via role.
2) Assume, we have one role and assigned to 100 users. This means root cause of risk for 100 users is this role.
3) Role gets risk from Profile. Auth objects and its values maintained in profile.
4) So, if we mitigate profile, user and role also mitigated.
5) If we mitigate role, users also will be mitigated

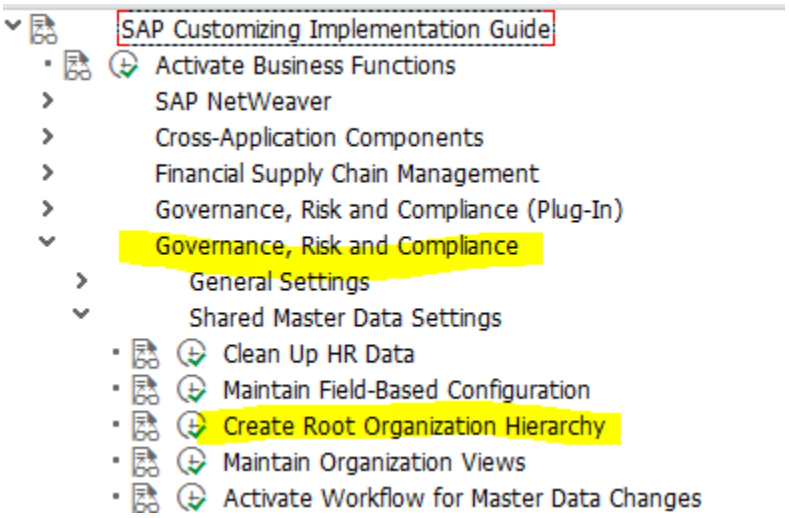
6) We can ignore Profile concept here as this concept does not exists now.
7) If we mitigate role, users who has this roles also be mitigated. No need to mitigate 100 users individually.
8) For one risk, there would be one mitigation id

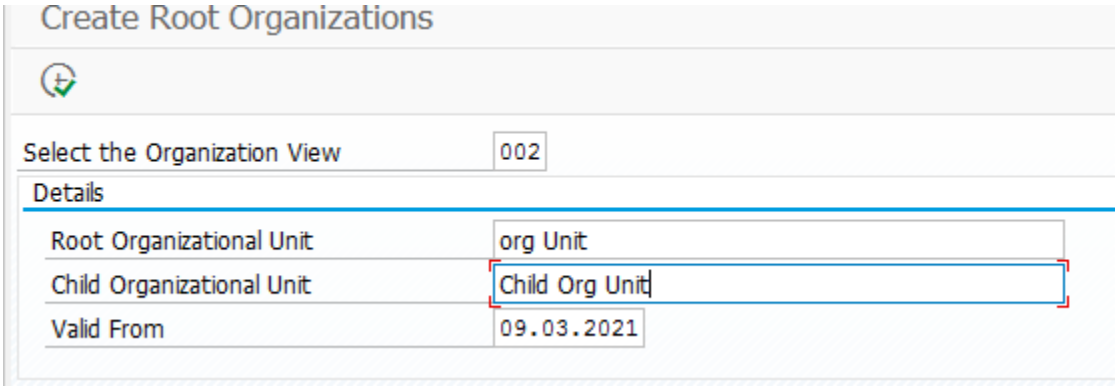


Mitigation Process:

1) Org Unit
2) Mitigation Approver
3) Mitigation Monitor
4) Maintain Approver and Monitor in Access Control Owners table
5) Maintain these users in Org Unit
6) Create Mitigation Control
7) Assign Mitigation Control to user/Role/Profile

- 1st we need to create Org Unit. Generally, its created by process control team.
- Created via SPRO.
- GRC---SPRO---SAP Reference IMG----GRC-----Shared Master Data Settings---Create Root Org Hierarchy.
- Every Organization will have its own Hierarchy
- Organization Hierarchy defined by Business Team.
- Its not our responsibility to create Org Unit.



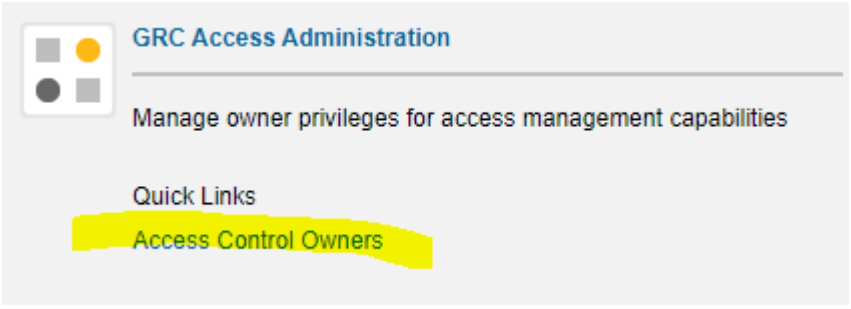


And execute...Now Org unit created (“ Route Created Successfully”)

2) Mitigation Approver & 3) Mitigation Monitor

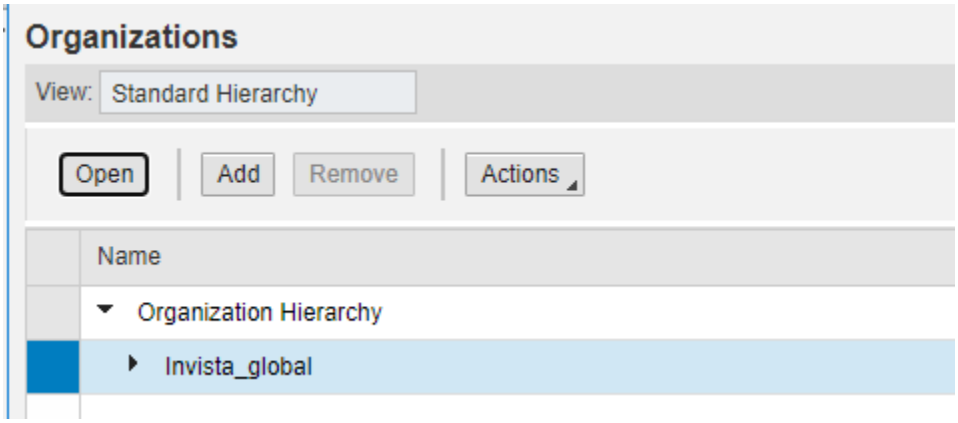
- Create 2 users in GRC
- Mitigation approver should have below roles in GRC
- DAIT_S_XXXX_SE_GRAC_END_USER
- SAP_GRAC_BASE
- SAP_GRAC_CONTROL_APPROVER
- SAP_GRAC_NWBC
- Mitigation approver is from Client
- Mitigation Controller should have below roles in GRC
- DAIT_S_XXXX_SE_GRAC_END_USER
- SAP_GRAC_BASE
- SAP_GRAC_NWBC
- SAP_GRAC_CONTROL_MONITOR

4) Maintain Approver and Monitor in Access Control Owners table

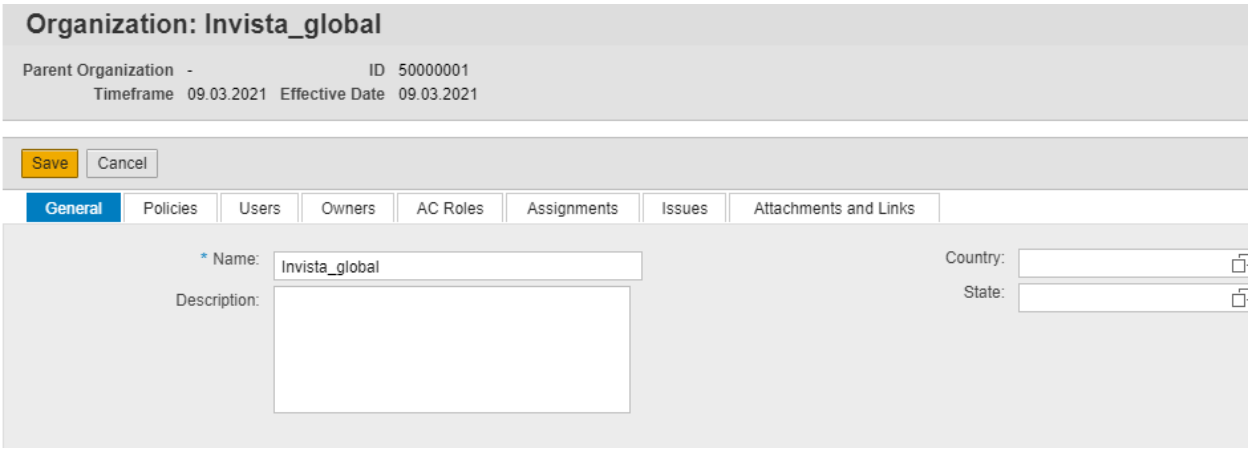


Create --- enter user name and select " Owner Type" and save

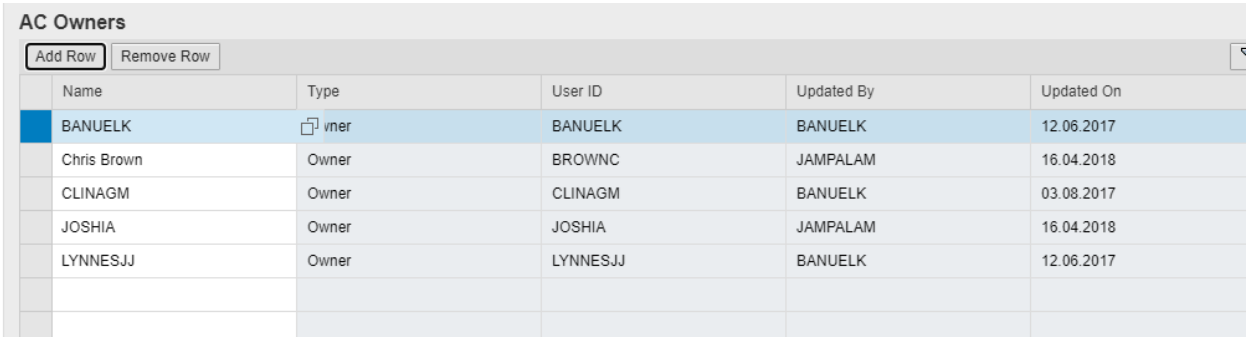
5) Maintain these users in Org Unit
   - GRC—NWBC---Setup---Organizations



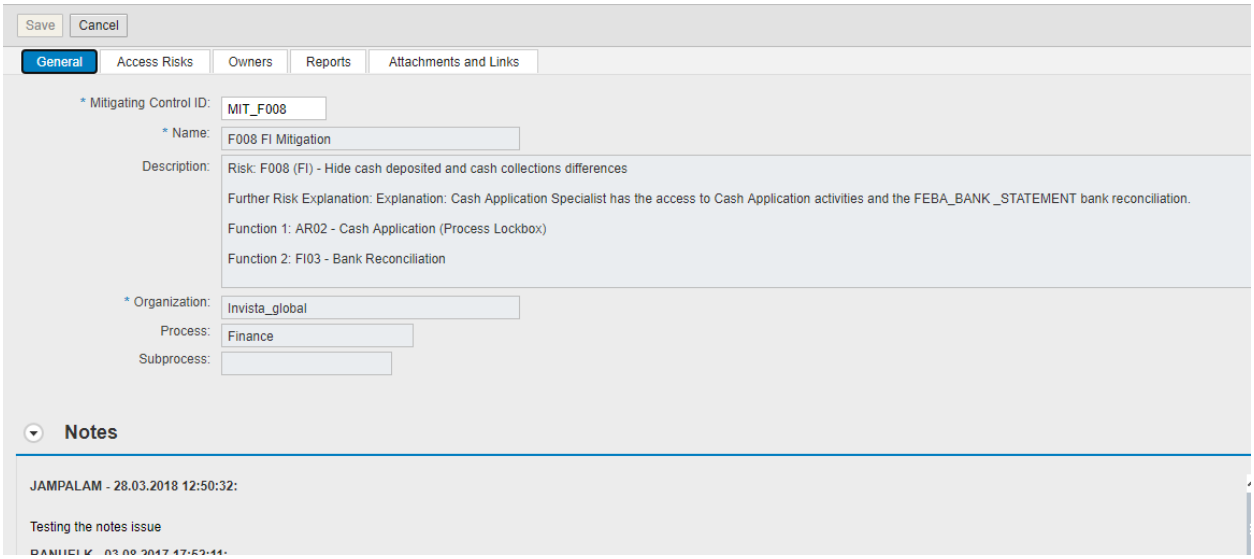
Select " Org Unit" and clieck on " Open and below screen comes.



Go to “ Owners”---Add row ---add user ids and save.

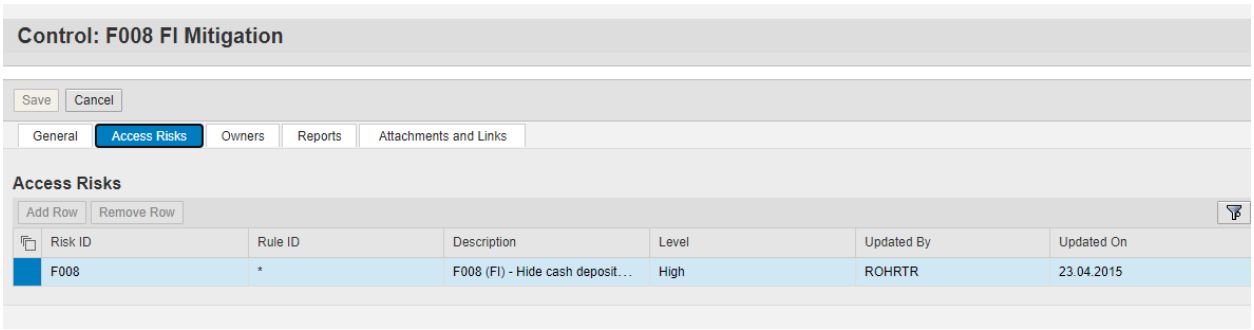


6) Create Mitigation Control
   - GRC---NWBC---SETP----Mitigation controls---Create

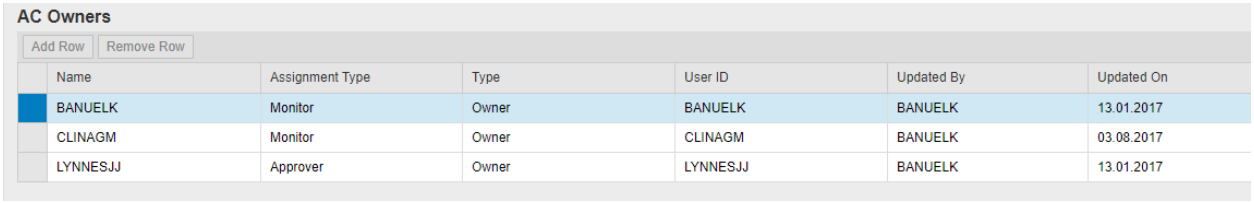


Go to “ Access Risks” (For which Access risk, we creating this Mitigation Control id..we need to maintain here)

We can maintain multiple risks for one Mitigation id.

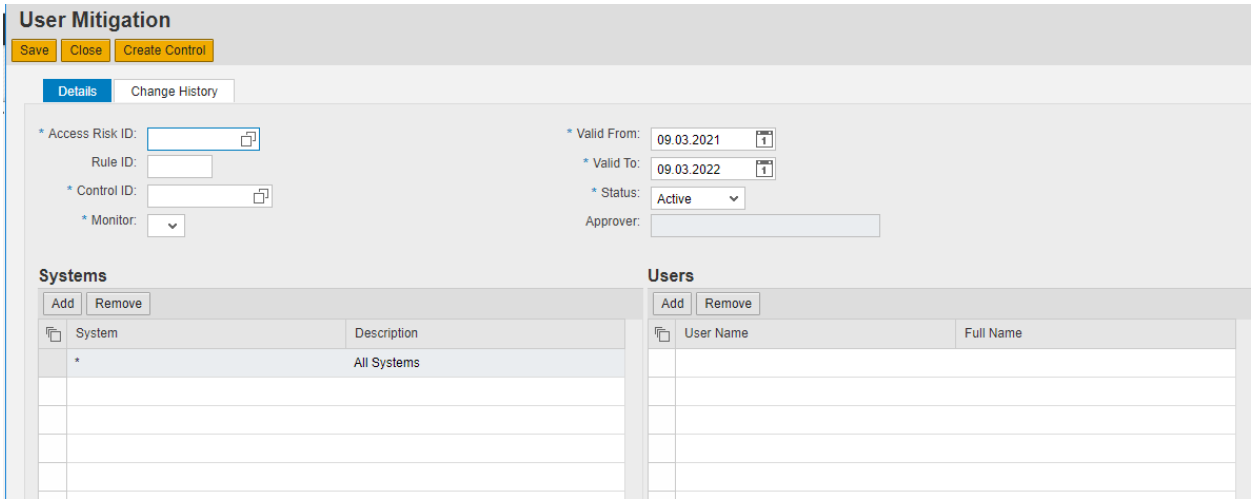


Go To Owners—Add user ids and save. We will get users lsi who ever maintained in “ Org Unit”



7) Assign Mitigation Control to user/Role/Profile

- When we run SOD for USER, we send the report to Business and Business will ask us to mitigate user.
- We can mitigate users from” Access Management” work center where as we can create Mitigation Controls from SETUP
- Access Management---Mitigated users----Assign



Ex:

Based on Risk id we select, then associate “ Mitigation control id “ will be appear

Now, Monitor and approver automatically selected.

Go to users—Add ---user id…save (We can see “ Submit “ button inplace of save once we configure MSMP

Once we submit, request goes to approver, once he approves, user will be mitigated.

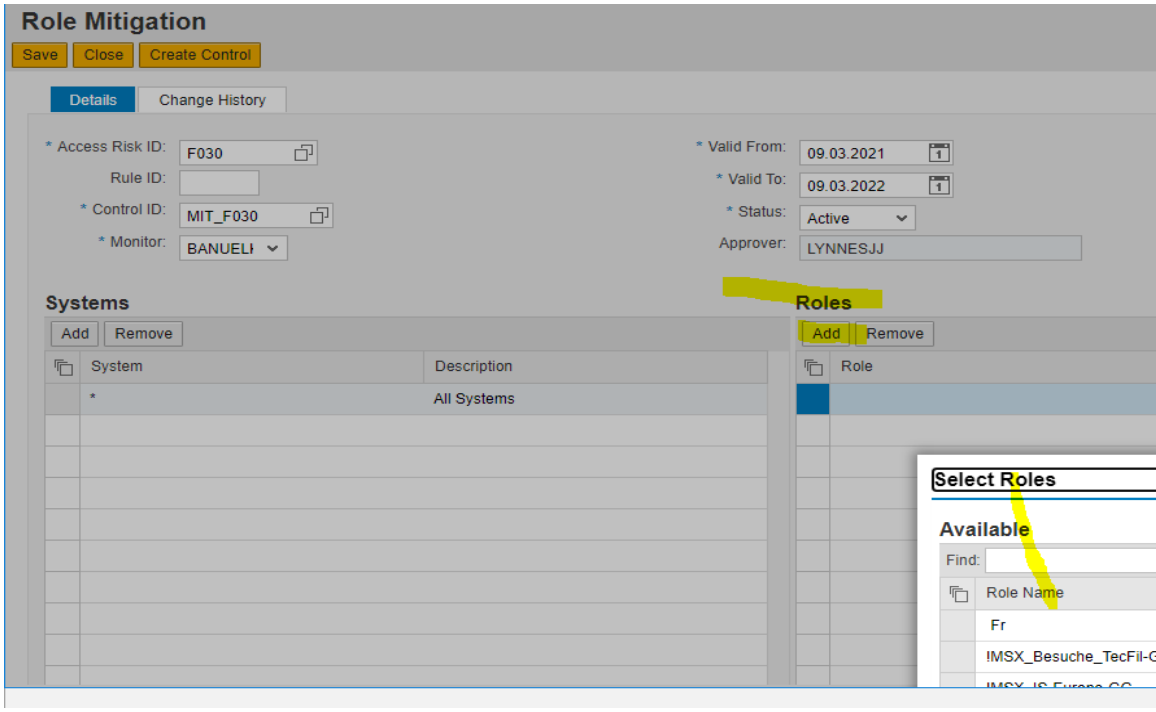
Now run the risk analysis for this user and we do not get any risks now.

Note: When I am performing Risk analysis, I found no risks to user. But , how should I know this user actually has risk but mitigated

Simple wat, user has risk but mitigated.---Select “ Include Mitigated Risks”

Mitigate Role:

- Access Management---Mitigated Roles----Assign
- Select the risk id, respective " Control id, will be populate
- Go to Roles and select role and save.
- Now role is mitigated.
-



(We can see " **Submit** " button in place of **save** once we configure MSMP)

- Now, run risk analysis for this mitigated role and we don't get any risks.

Critical Action

- Take a list of all T-codes which are critical. For ex, RZ10, STMS, SE01, SE38
- Put all these in one function(Access Rule Maintenance----Functions---Create---Add T-Codes.)

- Now , we need to define this function as “Critical action”.(Access Rule Maintenance----Access Risks---Create) and Risk Type should be “ Critical Action” and Risk Level” Critical”
- 3 types of risks we have SOD risk, Critical Action, Critical Permission.
- Combination of multiple function cause SOD. It can be 2 functions, 5….100.
- Combination of mutile T-codes is called SOD risk
- In Simple, SOD risk is of MIN 2 T-codes
- Critical Action: There are Few T-codes which are very critical and if we don’t want assign these to end users, then we can define those as critical
- Once you create a Risk, it has to be generated.
- Select the risk –Generate the rules. And confirm and close.
- Now, perform Risk Analysis. Select “ Critical Action”

Critical Permission:

- Take a list of all Auth Objects which are critical. For ex S_DEVELOP, S_TABU_DIS
- Put all these in one function(Access Rule Maintenance----Functions---Create)
- Go to permission and select Permission Group(T-code)
- We can not simply define permissions. We need to enter T-code in “ Permission Grop” , now respective Auth objects will be shown in “ Permission” Tab and maintain vales and save.
- Now we need to define this function as “ Critical Permission”
- Access Rule Maintenance----Access Risks---Create and Risk Type” Critical Permission”
- If we select risk type” SOD Risk” below error will come.
- SOD Risk ****must have at least 2 conflicting functions.
- Generate this risk.
- Run Risks analysis and select “ Critical Permission”

Critical Role:

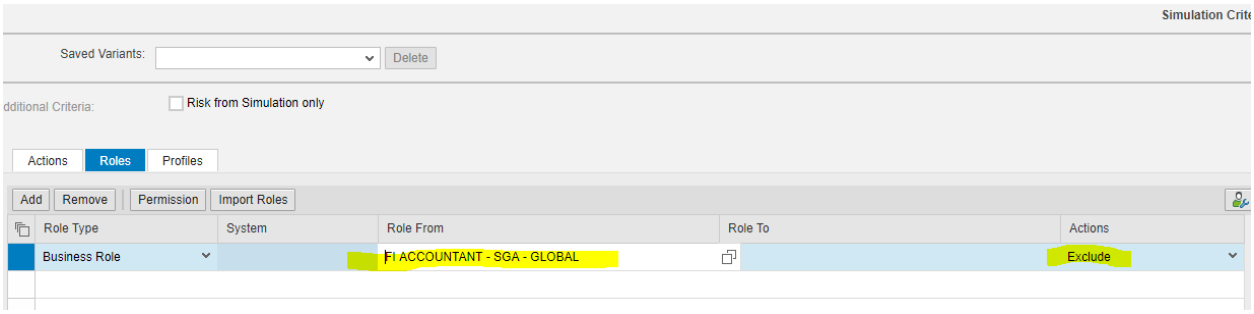
- Role which has sensitive data/Critical T-codes.
- We need to define this as “Critical Role” Now.
- Setup---Critical Access Rules----Critical role---Create----fill in all required fields
- Now, role is defined as “Critical role”
- Now, run Risks Analysis.
- We will get how many users has “Critical Role”

Critical Profile:

- As we know, SAP_ALL is a critical Profile
- Setup---Critical Access Rules----Critical Profile---Create----fill in all required fields
- Now, role is defined as “Critical role”
- Now, run Risks Analysis.
- We will get how many users has “Critical Profile.”

Remediation

- When we perform risks analysis and we found a risk and removing this risk from user is called “Remediation”.
- Removing the risk from user/Role/Profile is called “Remediation”
- There is no automatic process for Remediation. We need to do it manually.
- Mitigation is a automatic process.
- When we assign Mitigation controls to user, user will be mitigated automatically.
- We can use “ARM” for remediation. We can raise request via ARM to remove conflict access.
- Either we can remove entire role from user or Conflicting T-codes from user to make risk free.
- We can do this via testing with “exclude Values” in 2nd screen of “ User level Simulation”
- Ex: We maintained su01, pfcg commination as a risk. User has these 2 T-codes and got risk.
- In user level simulation, go to 2nd screen and add su01/Pfcg and select su01/pfcg in “ACTIONS” and select exclude and run it and we don’t get Any risk. Which means if we remove either su01/pfcg from user, user will not get risk. So if Business ok, we can modify role and move to prod.



Simulation:

- Simulation is nothing but Testing.
- Based on Simulation report, we need to decide how we are going to remediate user.
- Means, we need to remove role/T-code from user. T-code removal means removing T-code from user role.

Critical Role

- Define one role as a Critical role.
- Setup---Critical role---Create----fill in all required fields and save.
- Now, we have informed GRC system that one role(ZROLE) is critical role.
- Now, perform risk analysis at user level and check box Critical role/Profile. Run in Foreground.
- Now, we will list of all user who has critical role ZROLE

Critical Role

- Define one Profile as a Critical Profile.
- Setup---Critical Profile---Create----fill in all required fields and save
- Now, we have informed GRC system that one Profile(SAP_ALL) is critical Profile.
- Now, perform risk analysis at **user level** and check box Critical role/Profile. Run in Foreground.

- Now, we will list of all user who has critical Profile SAP_ALL

If you run risk analysis at **role level** and check box is “Critical role/Profile, we will get the list of all “Critical roles”

Critical Action: (Check box in Risk Analysis**)**

- How to get users list who has access to “Critical Actions”
- 1st we need to define what are critical actions.
- Create a **function** add T-codes which are critical like RZ10, SM30
- Create a risk and risk **type** should be “Critical Action” (Not SOD) and add this **function**
  and Risk level “Critical” and save.

  Generate the risk

  Now run risk analysis at user level and check box should be “Critical Action” and run in foreground.
  We will list of user who has access to “Critical Actions”.

  Note: User need not to have all T-codes which are critical. Any of the T-codes he has, we will get in output.

  For ex: We have defined, RZ10, Sm30 are critical actions, if a user has access to RZ10.
  When we run a risk analysis at user level with ” critical action”…..We will get this user id.

Critical Permission:

- Go to Permission
- We need to add Permission group (T-code) and enter Auth Objs in " Permission" and change the status to " Active"
- Define this as " Critical Permission"
- Access Risks---Create ----Fill in all required fields.
- Risk type should be " Critical Permission" and Risk level is " Critical" and Add functions and save.
- Generate this risk now.
- Run risk analysis at user level with " Critical Permission" check box
- We will get users list who has access to Critical permissions

EAM (Emergency Access Management)

- The Purpose of EAM is, we provide additional access to users(End users+ IT Users)
- For ex, you are in Finance department and you have a role by which you perform your regular activities.
- But there us requirement that you need to perform additional activities for which you don't have access.
- This additional access can be provided via FF
- We have 4 type of users in EAM.
    1. Fire Fighter Dialogue user in GRC (UPPALAVE)
    2. FF Id Reference user in ECC (E_FFSC_GBL0)
    3. FF Owner Dialogue user in GRC (Evandro)
    4. FF Controller Dialogue user in GRC

FireFighter: User who seeks additional access. Why we are creating this user in GRC:
Ans: This user needs to come to GRC and from GRC he perform additional activities in ECC

Role: SAP_GRAC_SUPER_USER_MGMT_USER ?? + 3 Basic roles

FF Id: Is a ID which has additional access. We will give this to FireFighter.
We create this user in ECC/Backend system
Once we create this user id in ECC, we need synch this user id in GRC

Once created , bring this user to GRC with " Repository Job Synch"

Role: The role which maintained in " Configuration settings" in 4010
We don't need to assign other Basic roles because, its not GRC user. Its ECC user

Now if you want provide any additional access, please provide that role to FFID in ECC.

For Ex: If its Finance FFID, assign all finance related access.

Ex: SAP_GRAC_SPM_FFID (This maintained in 4010 parameter)

FF Owner: For each FF ID, there must be on FF owner
Responsible to assign/approve this FF id to FireFighter
We need to map this owner id to FF id which means he will be owner for FFID.(Access Control Owners)

Role: SAP_GRAC_SUPER_USER_MGMT_OWNER

FF Controller: As we are giving additional access to FireFighter, we don't know what activities he performs in ECC via FFID. So there must be one person who should monitor this FireFighter activities.

We need to assign/Map this FF Controller to FF ID which means he is responsible to monitor activates done by FFID.
What ever FF does, notification will go to Controller.

Role: SAP_GRAC_SUPER_USER_MGMT_CNTLR

We need to check few Configuration Settings.
GRC—SPRO---SAP Reference IMG----GRC----AC----Maintain Configuration Settings

- All EAM related parameters available in parameter Group “EAM”
- There are 2 Parameters which are mandatory(4000, 4010)
- Application Type :4000
- User ID
- Role.
- How you want to provide additional access to FireFighter.
- Via User ID/ Role
- Please select User ID which means Via FFID we are providing additional access to Users.
- Which is also called “Centralized EAM”
- From GRC, we are maintaining this entire EAM Process.
- If you select “role” in App type, we don’t need to create FireFighter Id, we can have 1 role in ECC and assign to user via ARM

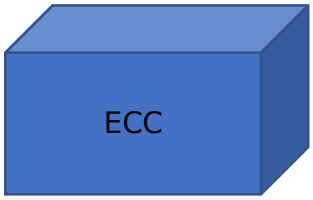
ID based EAM is called “ Centralized EAM”.
Role based EAM is called “ De centralized EAM”
3 users in GRC, 1 user in ECC(FFID)
FF Owner and FF Controller needs to maintained in Access Control Owners
FF Role Owner in Access Control Owners: For De Centralized EAM, we need to select “ FF Role Owner”

The second mandatory parameter is 4010 (FFID Role Name).

- If we are defining app type is “ User id”, we need to define what should be role needs to be assigned to FFID.
- Role for FF ID is “SAP_GRAC_SPM_FFID” maintain this in 4010
- Now, we need to assign role to FFID in ECC.
- Which means what ever user has this role is FFID.
- You can maintain any required role in 4010. But a user who has this role is called FFID.
- We have other parameters as well apart from 4000, 4010. Based on our requirement, we will maintain those.
- We can maintain FF Id validity 4001
- Send email immediately: Email will be sent immediately to Owner and Controller. (4002)
- Retrieve Logs: 4003, 4004, 4005
  This logs will be retrieved from ECC to GRC.

- Once User Id created in GRC (FF, Owner, Controller), ECC(FF ID), we have to assign Owner and Controller to FFID.
- NWBC---SETUP---we have 2 options. Super User Assignment and Super User Maintenance
- **Super User Assignment:** FF Owners can be assigned to FFID via this option
- **Super User Maintenance:** FF Controllers can be assigned to FFID via this option
- **Super User Maintenance:** Firefighters can be assigned via this option?????Why this step??

Param ID	Parm Group	Description
4000	06	Application type
4001	06	Default Firefighter Validity Period (Days)
4002	06	Send Email Immediately
4003	06	Retrieve Change Log
4004	06	Retrieve System log
4005	06	Retrieve Audit log
4006	06	Retrieve OS Command log
4007	06	Send Log Report Execution Notification Immediately
4008	06	Send FirefightId Login Notification
4009	06	Log Report Execution Notification
4010	06	Firefighter ID role name
4012	06	Default users for forwarding the Audit Log workflow
4013	06	Firefighter ID owner can submit request for Firefighter ID owned
4014	06	Firefighter ID controller can submit request for Firefighter ID controlled
4015	06	Enable Decentralized Firefighting
4017	06	Enable CUP request no to be shown in Firefighter - Firefighter ID/Role assgnm
4018	06	Enable detailed logging (SLG1) for EAM Log Synchronization programs



Create 3 users (FireFighter, FF Owner, FF Controller) in GRC and assign respective roles.
Create a user id(FF ID) in ECC and assign respective role.
Get this user to GRC with " Repository Job Synch
Maintain FF Owner, FF Controllers in " Access Control Owners"
Assign FFID to Owner, Controller, FireFighter
FireFighter perform some additional activities with FF Id
Notifications should go to Controller.
Controller can login to GRC...NWBC----" Reports & Analytics"---we have many kind of reports.

Go to " FF Log Summary Report"-----" Session Details" (If we don't get proper report, " FireFIghter Log Synch not done. Ge this done from GRC-----SPRO---GRC__AC----"Synch Jobs"----FF Log Synch"